Vulnerability Summary for the Week of June 17, 2019

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by Ug-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of Ug-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
actiontec -- t2200h_firmware	An issue was discovered on Actiontec T2200H T2200H-31.128L.08 devices, as distributed by Telus. By attaching a UART adapter to the UART pins on the system board, an attacker can use a special key sequence (Ctrl-\) to obtain a shell with root privileges. After gaining root access, the attacker can mount the filesystem read-write and make permanent modifications to the device including bricking of the device, disabling vendor management of	2019-06-17	7.2	CVE-2019-12789 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the device, preventing automatic upgrades, and permanently installing malicious code on the device.			
advantech -- webaccess	Stack-based buffer overflow in Advantech WebAccess/SCADA 8.4.0 allows a remote, unauthenticated attacker to execute arbitrary code by sending a crafted IOCTL 10012 RPC call.	2019-06-18	7.5	CVE-2019-3953 MISC
advantech -- webaccess	Stack-based buffer overflow in Advantech WebAccess/SCADA 8.4.0 allows a remote, unauthenticated attacker to execute arbitrary code by sending a crafted IOCTL 81024 RPC call.	2019-06-18	7.5	CVE-2019-3954 MISC
arenam -- amgallery	SQL Injection exists in the AMGallery 1.2.3 component for Joomla! via the filter_category_id parameter.	2019-06-19	7.5	CVE-2018-17398 MISC MISC
bubblesoftapps -- bubbleupnp	In BubbleUPnP 0.9 update 30, the XML parsing engine for SSDP/UPnP functionality is vulnerable to an XML External Entity Processing (XXE) attack. Remote, unauthenticated	2019-06-19	7.5	CVE-2018-15506 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers can use this vulnerability to: (1) Access arbitrary files from the filesystem with the same permission as the user account running BubbleUPnP, (2) Initiate SMB connections to capture a NetNTLM challenge/response and crack the cleartext password, or (3) Initiate SMB connections to relay a NetNTLM challenge/response and achieve Remote Command Execution in Windows domains.			
bzip -- bzip2	BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.	2019-06-19	7.5	CVE-2019-12900 MISC
chronoscan -- chronoscan	SQL injection vulnerability in ChronoScan version 1.5.4.3 and earlier allows an unauthenticated attacker to execute arbitrary SQL commands via the wcr_machineid cookie.	2019-06-21	7.5	CVE-2018-15868 MISC MISC
cisco -- meeting_server	A vulnerability in the CLI configuration shell of Cisco Meeting Server could allow an authenticated, local attacker to inject arbitrary commands as the root user. The vulnerability is due to insufficient input	2019-06-19	7.2	CVE-2019-1623 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	validation during the execution of a vulnerable CLI command. An attacker with administrator-level credentials could exploit this vulnerability by injecting crafted arguments during command execution. A successful exploit could allow the attacker to perform arbitrary code execution as root on an affected product.			
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, the BACnet daemon does not properly validate input, which could allow a remote attacker to send specially crafted packets causing the device to become unavailable.	2019-06-18	7.8	CVE-2018-18878 MISC MISC
deltaww -- devicenet_builder	Delta Electronics DeviceNet Builder 2.04 has a User Mode Write AV starting at image00400000+0x000000000017a45e.	2019-06-19	7.5	CVE-2019-12898 MISC
deltaww -- devicenet_builder	Delta Electronics DeviceNet Builder 2.04 has a User Mode Write AV starting at ntdll!RtlQueueWorkItem+0x0000000000005e3.	2019-06-19	7.5	CVE-2019-12899 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
education_website_project -- education_website	SQL injection exists in Scriptzee Education Website 1.0 via the college_list.html subject, city, or country parameter.	2019-06-19	7.5	CVE-2018-17840 MISC MISC
ethereum -- ethereumj	An issue was discovered in EthereumJ 1.8.2. There is Unsafe Deserialization in ois.readObject in mine/Ethash.java and decoder.readObject in crypto/ECKey.java. When a node syncs and mines a new block, arbitrary OS commands can be run on the server.	2019-06-20	10.0	CVE-2018-15890 MISC MISC MISC
f5 -- big-ip_access_policy_manager	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff.	2019-06-18	7.8	CVE-2019-11477 MISC MLIST MISC MISC MISC CONFIRM CONFIRM MISC CERT-VN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
flippa_marketplace_clone_project -- flippa_marketplace_clone	SQL injection exists in Scriptzee Flippa Marketplace Clone 1.0 via the site-search sortBy or sortDir parameter.	2019-06-19	7.5	CVE-2018-17841 MISC MISC
fusionpbx -- fusionpbx	app/backup/index.php in the Backup Module in FusionPBX 4.4.3 suffers from a command injection vulnerability due to a lack of input validation, which allows authenticated administrative attackers to execute commands on the host.	2019-06-17	9.0	CVE-2019-11410 MISC MISC
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a web user interface that allows a user to manage the device. As a part of the functionality the device firmware file contains a file known as relay.sh which allows the device to create relay ports and connect the device to Vera servers. This is primarily used as a method of communication between the device and Vera servers so the devices can be communicated with even when the user is not at home. One of the parameters retrieved by this specific script is "remote_host". This parameter is not sanitized by the script	2019-06-17	9.0	CVE-2017-9384 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	correctly and is passed in a call to "eval" to execute another script where remote_host is concatenated to be passed a parameter to the second script. This allows an attacker to escape from the executed command and then execute any commands of his/her choice.			
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a web user interface that allows a user to manage the device. As a part of the functionality the device firmware file contains a file known as proxy.sh which allows the device to proxy a specific request to and from from another website. This is primarily used as a method of communication between the device and Vera website when the user is logged in to the https://home.getvera.com and allows the device to communicate between the device and website. One of the parameters retrieved by this specific script is "url". This parameter is not sanitized by the script correctly and is passed in a call to "eval" to execute "curl" functionality. This allows an attacker to escape from the	2019-06-17	9.0	CVE-2017-9388 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	executed command and then execute any commands of his/her choice.			
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a web user interface that allows a user to manage the device. As a part of the functionality the device allows a user to install applications written in the Lua programming language. Also the interface allows any user to write his/her application in the Lua language. However, this functionality is not protected by authentication and this allows an attacker to run arbitrary Lua code on the device. The POST request is forwarded to LuaUPNP daemon on the device. This binary handles the received Lua code in the function "LU::JobHandler_LuaUPnP::RunLua(LU::JobHandler_LuaUPnP *__hidden this, LU::UPnPActionWrapper *)". The value in the "code" parameter is then passed to the function "LU::LuaInterface::RunCode(char const*)" which actually loads the Lua engine and runs the code.	2019-06-17	9.0	CVE-2017-9389 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "request_image" as one of the service actions for a normal user to retrieve an image from a camera that is controlled by the controller. It seems that the "URL" parameter passed in the query string is not sanitized and is stored on the stack which allows an attacker to overflow the buffer. The function "LU::Generic_IP_Camera_Manager::REQ_Image" is activated when the lu_request_image is passed as the "id" parameter in query string. This function then calls "LU::Generic_IP_Camera_Manager::GetUrlFromArguments" and passes a "pointer" to the function where it will be allowed to store the value from the URL parameter. This pointer is passed as the second parameter $a2 to the function "LU::Generic_IP_Camera_Manager::GetUrlFromArguments". However, neither the callee or the caller in this case performs a simple length check and as a	2019-06-17	9.0	CVE-2017-9391 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	result an attacker who is able to send more than 1336 characters can easily overflow the values stored on the stack including the $RA value and thus execute code on the device.			
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "request_image" as one of the service actions for a normal user to retrieve an image from a camera that is controlled by the controller. It seems that the "res" (resolution) parameter passed in the query string is not sanitized and is stored on the stack which allows an attacker to overflow the buffer. The function "LU::Generic_IP_Camera_Manager::REQ_Image" is activated when the lu_request_image is passed as the "id" parameter in the query string. This function then calls "LU::Generic_IP_Camera_Manager::GetUrlFromArguments". This function retrieves all the parameters passed in the query	2019-06-17	9.0	CVE-2017-9392 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	string including "res" and then uses the value passed in it to fill up buffer using the sprintf function. However, the function in this case lacks a simple length check and as a result an attacker who is able to send more than 184 characters can easily overflow the values stored on the stack including the $RA value and thus execute code on the device.			
google -- android	In llcp_util_parse_connect of llcp_util.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-111660010	2019-06-19	7.1	CVE-2018-9561 MISC
google -- android	In llcp_util_parse_cc of llcp_util.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for	2019-06-19	7.1	CVE-2018-9563 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-114237888			
google -- android	In llcp_util_parse_link_params of llcp_util.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-114238578	2019-06-19	7.1	CVE-2018-9564 MISC
google -- android	In findAvailSpellCheckerLocked of TextServicesManagerService.java, there is a possible way to bypass the warning dialog when selecting an untrusted spell checker due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2	2019-06-19	7.2	CVE-2019-1985 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Android-8.0Android ID: A-118694079			
google -- android	In ih264d_fmt_conv_420sp_to_420p of ih264d_format_conv.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118399205	2019-06-19	9.3	CVE-2019-1989 MISC
google -- android	In ihevcd_fmt_conv_420sp_to_420p of ihevcd_fmt_conv.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118453553	2019-06-19	9.3	CVE-2019-1990 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In addLinks of Linkify.java, there is a possible phishing vector due to an unusual root cause. This could lead to remote code execution or misdirection of clicks with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-116321860	2019-06-19	9.3	CVE-2019-2003 MISC
google -- android	In serviceDied of HalDeathHandlerHidl.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege in the audio server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9Android ID: A-116665972	2019-06-19	10.0	CVE-2019-2006 MISC
google -- android	In getReadIndex and getWriteIndex of FifoControllerBase.cpp, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege in the audio server with no additional execution	2019-06-19	10.0	CVE-2019-2007 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-120789744			
google -- android	In createEffect of AudioFlinger.cpp, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-122309228	2019-06-19	7.6	CVE-2019-2008 MISC
google -- android	In l2c_lcc_proc_pdu of l2c_fcr.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120665616	2019-06-19	8.3	CVE-2019-2009 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In phNxpNciHal_process_ext_rsp of phNxpNciHal_ext.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118152591	2019-06-19	7.2	CVE-2019-2010 MISC
google -- android	In readNullableNativeHandleNoDup of Parcel.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-120084106	2019-06-19	7.2	CVE-2019-2011 MISC
google -- android	In rw_t3t_act_handle_fmt_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution	2019-06-19	9.3	CVE-2019-2012 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120497437			
google -- android	In rw_t3t_act_handle_sro_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120497583	2019-06-19	9.3	CVE-2019-2013 MISC
google -- android	In rw_t3t_handle_get_sc_poll_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2	2019-06-19	9.3	CVE-2019-2014 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Android-8.0 Android-8.1 Android-9Android ID: A-120499324			
google -- android	In rw_t3t_act_handle_check_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120503926	2019-06-19	9.3	CVE-2019-2015 MISC
google -- android	In NFA_SendRawFrame of nfa_dm_api.cc, there is a possible out-of-bound write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120664978	2019-06-19	9.3	CVE-2019-2016 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-121035711	2019-06-19	7.2	CVE-2019-2017 MISC
google -- android	In resetPasswordInternal of DevicePolicyManagerService.java, there is a possible bypass of password reset protection due to an unusual root cause. Remote user interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-110172241	2019-06-19	9.3	CVE-2019-2018 MISC
google -- android	In ce_t4t_data_cback of ce_t4t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0	2019-06-19	7.1	CVE-2019-2019 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-115635871			
google -- android	In llcp_dlc_proc_rr_rnr_pdu of llcp_dlc.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-116788646	2019-06-19	7.1	CVE-2019-2020 MISC
google -- android	In rw_t3t_act_handle_ndef_detect_rsp of rw_t3t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120428041	2019-06-19	7.1	CVE-2019-2021 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In rw_t3t_act_handle_fmt_rsp and rw_t3t_act_handle_sro_rsp of rw_t3t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120506143	2019-06-19	7.1	CVE-2019-2022 MISC
google -- android	In ServiceManager::add function in the hardware service manager, there is an insecure permissions check based on the PID of the caller. This could allow an app to add or replace a HAL service with its own service, gaining code execution in a privileged process.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-121035042Upstream kernel	2019-06-19	7.2	CVE-2019-2023 MISC
google -- android	In em28xx_unregister_dvb of em28xx-dvb.c, there is a possible use after free issue. This could lead to local escalation of privilege with no additional execution privileges needed.	2019-06-19	7.2	CVE-2019-2024 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-111761954References: Upstream kernel			
google -- android	In binder_thread_read of binder.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-116855682References: Upstream kernel	2019-06-19	7.2	CVE-2019-2025 MISC
healthnode_hospital_management_system_project -- healthnode_hospital_management_system	SQL Injection exists in HealthNode Hospital Management System 1.0 via the id parameter to dashboard/Patient/info.php or dashboard/Patient/patientdetails.php.	2019-06-19	7.5	CVE-2018-17393 MISC MISC
hotel_booking_engine_project -- hotel_booking_engine	SQL injection exists in Scriptzee Hotel Booking Engine 1.0 via the hotels h_room_type parameter.	2019-06-19	7.5	CVE-2018-17842 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- control_desk	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbirary commands on the system. IBM X-Force ID: 161680.	2019-06-19	8.5	CVE-2019-4364 XF CONFIRM
ibm -- tivoli_netcool/impact	IBM Tivoli Netcool/Impact 7.1.0 allows for remote execution of command by low privileged User. Remote code execution allow to execute arbitrary code on system which lead to take control over the system. IBM X-Force ID: 158094.	2019-06-17	7.7	CVE-2019-4103 XF CONFIRM
infoblox -- nios	A privilege escalation vulnerability in the "support access" feature on Infoblox NIOS 6.8 through 8.4.1 could allow a locally authenticated administrator to temporarily gain additional privileges on an affected device and perform actions within the super user scope. The vulnerability is due to a weakness in the "support access" password generation algorithm. A locally authenticated administrative user may be able to exploit this vulnerability if the "support access" feature is enabled, they know the support access code for the current session, and they	2019-06-17	7.2	CVE-2018-10239 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	know the algorithm to generate the support access password from the support access code. "Support access" is disabled by default. When enabled, the access will be automatically disabled (and support access code will expire) after the 24 hours.			
jimtawl_project -- jimtawl	SQL Injection exists in the Jimtawl 2.2.7 component for Joomla! via the id parameter.	2019-06-19	7.5	CVE-2018-17399 MISC MISC
libgd -- libgd	The GD Graphics Library (aka libgd) through 2.2.5 has a Double Free Vulnerability in the gdImageBmpPtr function.	2019-06-20	7.5	CVE-2018-15878 MISC
libgd -- libgd	The GD Graphics Library (aka libgd) through 2.2.5 has a Double Free Vulnerability in the gdImageBmpPt function.	2019-06-20	7.5	CVE-2018-15879 MISC
linux -- linux_kernel	A flaw was found in the Linux kernel. A heap based buffer overflow in mwifiex_uap_parse_tail_ies function in	2019-06-14	7.5	CVE-2019-10126 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	drivers/net/wireless/marvell/mwifiex/ie.c might lead to memory corruption and possibly other consequences.			CONFIRM MLIST MLIST BUGTRAQ DEBIAN
linux -- linux_kernel	A double-free can happen in idr_remove_all() in lib/idr.c in the Linux kernel 2.6 branch. An unprivileged local attacker can use this flaw for a privilege escalation or for a system crash and a denial of service (DoS).	2019-06-18	7.2	CVE-2019-3896 BID CONFIRM
onapp -- onapp	OnApp before 5.0.0-88, 5.5.0-93, and 6.0.0-196 allows an attacker to run arbitrary commands with root privileges on servers managed by OnApp for XEN/KVM hypervisors. To exploit the vulnerability an attacker has to have control of a single server on a given cloud (e.g. by renting one). From the source server, the attacker can craft any command and trigger the OnApp platform to execute that command with root privileges on a target server.	2019-06-19	8.5	CVE-2019-12491 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
open-xchange -- open-xchange_appsuite	OX App Suite 7.10.0 and earlier has Incorrect Access Control.	2019-06-17	7.5	CVE-2019-7158 MISC
open_faculty_evaluation_system_project -- open_faculty_evaluation_system	Open Faculty Evaluation System 5.6 for PHP 5.6 allows submit_feedback.php SQL Injection, a different vulnerability than CVE-2018-18758.	2019-06-19	7.5	CVE-2018-18757 MISC MISC
open_faculty_evaluation_system_project -- open_faculty_evaluation_system	Open Faculty Evaluation System 7 for PHP 7 allows submit_feedback.php SQL Injection, a different vulnerability than CVE-2018-18757.	2019-06-19	7.5	CVE-2018-18758 MISC MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and	2019-06-19	7.5	CVE-2019-2729 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
ranksol -- twilio_web_to_fax_machine_system	SQL Injection exists in Twilio WEB To Fax Machine System 1.0 via the email or password parameter to login_check.php, or the id parameter to add_email.php or edit_content.php.	2019-06-19	7.5	CVE-2018-17388 MISC MISC
sahipro -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7.x.x and 8.0.0. A parameter in the web reports module is vulnerable to h2 SQL injection. This can be exploited to inject SQL queries and run standard h2 system functions.	2019-06-17	7.5	CVE-2018-20469 MISC MISC
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of changing the administrative password for the web management interface. It seems that the device does not implement any cross site request forgery protection mechanism which allows an attacker to trick a user who is logged in to the web management interface to	2019-06-18	9.3	CVE-2017-8328 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	change a user's password. Also this is a systemic issue.			
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of adding new routes to the device. It seems that the POST parameters passed in this request to set up routes on the device can be set in such a way that would result in passing commands to a "popen" API in the function and thus result in command injection on the device. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "dest" is extracted at address 0x00420FC4. The POST	2019-06-18	9.0	CVE-2017-8333 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter "dest is concatenated in a route add command and this is passed to a "popen" function at address 0x00421220. This allows an attacker to provide the payload of his/her choice and finally take control of the device.			
sophos -- sfos	A shell escape vulnerability in /webconsole/Controller in Admin Portal of Sophos XG firewall 17.0.8 MR-8 allow remote authenticated attackers to execute arbitrary OS commands via shell metacharacters in the "dbName" POST parameter.	2019-06-20	9.0	CVE-2018-16117 CONFIRM MISC MISC
thephpfactory -- auction_factory	SQL Injection exists in the Auction Factory 4.5.5 component for Joomla! via the filter_order_Dir or filter_order parameter.	2019-06-19	7.5	CVE-2018-17374 MISC MISC
thephpfactory -- dutch_auction_factory	SQL Injection exists in the Dutch Auction Factory 2.0.2 component for Joomla! via the filter_order_Dir or filter_order parameter.	2019-06-19	7.5	CVE-2018-17381 MISC MISC
thephpfactory -- micro_deal_factory	SQL Injection exists in the Micro Deal Factory 2.4.0 component for Joomla! via the id	2019-06-19	7.5	CVE-2018-1738

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter, or the PATH_INFO to mydeals/ or listdeals/.			6 MISC MISC
tp-link -- tl-wr1043nd_firmware	An issue was discovered on TP-Link TL-WR1043ND V2 devices. An attacker can send a cookie in an HTTP authentication packet to the router management web interface, and fully control the router without knowledge of the credentials.	2019-06-19	10.0	CVE-2019-6971 MISC MISC
videolan -- vlc_media_player	An issue was discovered in zlib_decompress_extra in modules/demux/mkv/util.cpp in VideoLAN VLC media player 3.x through 3.0.7. The Matroska demuxer, while parsing a malformed MKV file type, has a double free.	2019-06-18	7.5	CVE-2019-12874 MISC
webmin -- webmin	In Webmin through 1.910, any user authorized to the "Package Updates" module can execute arbitrary commands with root privileges via the data parameter to update.cgi.	2019-06-15	9.0	CVE-2019-12840 MISC BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
westerndigital -- my_book_live_firmware	Western Digital WD My Book Live (all versions) has a root Remote Command Execution bug via shell metacharacters in the /api/1.0/rest/language_configuration language parameter. It can be triggered by anyone who knows the IP address of the affected device.	2019-06-19	10.0	CVE-2018-18472 MISC MISC
whatsapp -- whatsapp	When receiving calls using WhatsApp for iOS, a missing size check when parsing a sender-provided packet allowed for a stack-based overflow. This issue affects WhatsApp for iOS prior to v2.18.90.24 and WhatsApp Business for iOS prior to v2.18.90.24.	2019-06-14	7.5	CVE-2018-20655 BID MISC
whatsapp -- whatsapp	An out-of-bounds read was possible in WhatsApp due to incorrect parsing of RTP extension headers. This issue affects WhatsApp for Android prior to 2.18.276, WhatsApp Business for Android prior to 2.18.99, WhatsApp for iOS prior to 2.18.100.6, WhatsApp Business for iOS prior to 2.18.100.2, and WhatsApp for Windows Phone prior to 2.18.224.	2019-06-14	7.5	CVE-2018-6350 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zohocorp -- manageengine_adselfservice_plus	An authentication bypass vulnerability in the password reset functionality in Zoho ManageEngine ADSelfService Plus before 5.0.6 allows an attacker with physical access to gain a shell with SYSTEM privileges via the restricted thick client browser. The attack uses a long sequence of crafted keyboard input.	2019-06-17	7.2	CVE-2019-12476 BID MISC MISC
zohocorp -- manageengine_analytics_plus	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow	2019-06-18	7.2	CVE-2019-12133 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus.			

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
afian -- filerun	FileRun 2019.05.21 allows XSS via the filename to the ?module=fileman&section=do&page=up URI.	2019-06-20	4.3	CVE-2019-12905 MISC
alpinelinux -- abuild	Alpine Linux abuild through 3.4.0 allows an unprivileged member of the abuild group to add an untrusted package via a --keys-dir option that causes acceptance of an untrusted signing key.	2019-06-18	4.0	CVE-2019-12875 MISC MISC
alternate-tools -- alternate_pic_view	Alternate Pic View 2.600 has a User Mode Write AV starting at PicViewer!PerfgrapFinalize+0x00000000000a8868.	2019-06-19	5.0	CVE-2019-12893 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alternate-tools -- alternate_pic_view	Alternate Pic View 2.600 has a Read Access Violation at the Instruction Pointer after a call from PicViewer!PerfgrapFinalize+0x00000000000a9a1b.	2019-06-19	5.0	CVE-2019-12894 MISC
alternate-tools -- alternate_pic_view	In Alternate Pic View 2.600, the Exception Handler Chain is Corrupted starting at PicViewer!PerfgrapFinalize+0x00000000000b916d.	2019-06-19	5.0	CVE-2019-12895 MISC
apache -- allura	In Apache Allura prior to 1.11.0, a vulnerability exists for stored XSS on the user dropdown selector when creating or editing tickets. The XSS executes when a user engages with that dropdown on that page.	2019-06-18	4.3	CVE-2019-10085 BID MISC MLIST
artha_project -- artha	Artha ~ The Open Thesaurus 1.0.3.0 has a Buffer Overflow.	2019-06-18	5.0	CVE-2018-18944 MISC MISC
b3log -- solo	b3log Solo 2.9.3 has XSS in the Input page under the "Publish Articles" menu with an ID of "articleTags" stored in the "tag" JSON field, which allows remote attackers to inject arbitrary Web scripts or HTML via a carefully crafted site name in an admin-authenticated HTTP request.	2019-06-20	4.3	CVE-2018-16248 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- integrated_management_controller	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to access potentially sensitive system usage information. The vulnerability is due to a lack of proper data protection mechanisms. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow an attacker to view sensitive system data.	2019-06-19	5.0	CVE-2019-1631 BID CISCO
cisco -- prime_service_catalog	A vulnerability in the web-based management interface of Cisco Prime Service Catalog Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protection mechanisms on the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user.	2019-06-19	6.8	CVE-2019-1874 BID CISCO
cloudera -- data_science_workbench	An issue was discovered in Cloudera Data Science Workbench (CDSW) 1.2.x through 1.4.0.	2019-06-21	5.0	CVE-2018-15665

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Unauthenticated users can get a list of user accounts.			MISC CONFIRM
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, a readouts_rd.php directory traversal issue makes it possible to read any file present on the underlying operating system.	2019-06-18	5.0	CVE-2018-18876 MISC MISC
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, an authenticated web user can access an alternative configuration page config_main.php that allows manipulation of the device.	2019-06-18	6.5	CVE-2018-18877 MISC MISC
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, an authenticated web user can pipe commands directly to the underlying operating system as user input is not sanitized in networkdiags.php.	2019-06-18	6.5	CVE-2018-18879 MISC MISC
corel -- paintshop_pro_2019	An issue was discovered in Corel PaintShop Pro 2019 21.0.0.119. An integer overflow in the jp2 parsing library allows an attacker to overwrite memory and to execute arbitrary code.	2019-06-19	6.8	CVE-2019-6114 MISC
craftcms -- craft_cms	Craft CMS 3.1.30 has XSS.	2019-06-18	4.3	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				12823 MISC CONFIRM
creatiwity -- witycms	A "search for user discovery" injection issue exists in Creatiwity witycMS 0.6.2 via the "Utilisateur" menu. No input parameters are filtered, e.g., the /admin/user/users Nickname, email, firstname, lastname, and groupe parameters.	2019-06-20	4.0	CVE-2018-16251 MISC
debian -- debian_linux	An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.7, Community Edition 6.0.x through 6.0.19, and Community Edition 5.0.x through 5.0.36. An attacker could send a malicious email to an OTRS system. If a logged-in agent user quotes it, the email could cause the browser to load external image resources.	2019-06-17	4.3	CVE-2019-12248 CONFIRM MISC
dotcms -- dotcms	dotCMS before 5.1.6 is vulnerable to a SQL injection that can be exploited by an attacker of the role Publisher via view_unpushed_bundles.jsp.	2019-06-18	6.5	CVE-2019-12872 MISC MISC
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 and earlier allows XML External Entity Blind Injection, related to pingback.axd and	2019-06-21	5.0	CVE-2019-10718

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	BlogEngine.Core/Web/HttpHandlers/PingbackHandler.cs.			MISC MISC
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 and earlier allows Directory Traversal and Remote Code Execution because file creation is mishandled, related to /api/upload and BlogEngine.NET/AppCode/Api/UploadController.cs. NOTE: this issue exists because of an incomplete fix for CVE-2019-6714.	2019-06-21	6.5	CVE-2019-10719 MISC FULL DISC MISC
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 and earlier allows Directory Traversal and Remote Code Execution via the theme cookie to the File Manager. NOTE: this issue exists because of an incomplete fix for CVE-2019-6714.	2019-06-21	6.5	CVE-2019-10720 MISC FULL DISC MISC
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7 and earlier allows XXE via an apml file to syndication.axd.	2019-06-21	5.0	CVE-2019-11392 MISC
edrawsoft -- edraw_max	Edraw Max 7.9.3 has Heap Corruption starting at ntdll!RtlpNtMakeTemporaryKey+0x0000000000001a77.	2019-06-19	5.0	CVE-2019-12896 MISC
edrawsoft -- edraw_max	Edraw Max 7.9.3 has a Read Access Violation at the Instruction Pointer after a call from	2019-06-19	5.0	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ObjectModule!Paint::Clear+0x0000000000000074.			12897 MISC
exacq -- enterprise_system_manager	A vulnerability in the exacqVision Enterprise System Manager (ESM) v5.12.2 application whereby unauthorized privilege escalation can potentially be achieved. This vulnerability impacts exacqVision ESM v5.12.2 and all prior versions of ESM running on a Windows operating system. This issue does not impact any Windows Server OSs, or Linux deployments with permissions that are not inherited from the root directory. Authorized Users have ?modify? permission to the ESM folders, which allows a low privilege account to modify files located in these directories. An executable can be renamed and replaced by a malicious file that could connect back to a bad actor providing system level privileges. A low privileged user is not able to restart the service, but a restart of the system would trigger the execution of the malicious file. This issue affects: Exacq Technologies, Inc. exacqVision Enterprise System Manager (ESM) Version 5.12.2 and prior versions; This issue does not affect: Exacq Technologies, Inc. exacqVision Enterprise System Manager (ESM) 19.03 and above.	2019-06-18	6.9	CVE-2019-7588 CONFIRM MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
f5 -- big-ip_access_policy_manager	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e.	2019-06-18	5.0	CVE-2019-11478 MISC MISC MISC MISC CONFIRM CONFIRM MISC CERT-VN
f5 -- big-ip_access_policy_manager	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.	2019-06-18	5.0	CVE-2019-11479 BID MISC MISC MISC CONFIRM CONFIRM MISC CERT-VN
fasterxml -- jackson-databind	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x through 2.9.9. When Default Typing is enabled (either globally or for a specific property)	2019-06-19	4.3	CVE-2019-12814 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	for an externally exposed JSON endpoint and the service has JDOM 1.x or 2.x jar in the classpath, an attacker can send a specifically crafted JSON message that allows them to read arbitrary local files on the server.			MLIST MLIST MLIST MLIST MLIST
foxitsoftware -- foxit_pdf_sdk_activex	A use after free in the TextBox field Validate action in IReader_ContentProvider can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031. An attacker can leverage this to gain remote code execution. Relative to CVE-2018-19452, this has a different free location and requires different JavaScript code for exploitation.	2019-06-17	6.8	CVE-2018-19444 MISC
foxitsoftware -- foxit_pdf_sdk_activex	A command injection can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when the JavaScript API app.launchURL is used. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	CVE-2018-19445 MISC
foxitsoftware -- foxit_pdf_sdk_activex	A File Write can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when the JavaScript API	2019-06-17	6.8	CVE-2018-19446 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Doc.createDataObject is used. An attacker can leverage this to gain remote code execution.			
foxitsoftware -- foxit_pdf_sdk_activex	A stack-based buffer overflow can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) 5.4.0.1031 when parsing the URI string. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	CVE-2018-19447 MISC
foxitsoftware -- foxit_pdf_sdk_activex	In Foxit Reader SDK (ActiveX) Professional 5.4.0.1031, an uninitialized object in IReader_ContentProvider::GetDocEventHandler occurs when embedding the control into Office documents. By opening a specially crafted document, an attacker can trigger an out of bounds write condition, possibly leveraging this to gain remote code execution.	2019-06-17	6.8	CVE-2018-19448 MISC
foxitsoftware -- foxit_pdf_sdk_activex	A File Write can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when the JavaScript API Doc.exportAsFDF is used. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	CVE-2018-19449 MISC
foxitsoftware -- foxit_pdf_sdk_activex	A command injection can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) 5.4.0.1031 when parsing a launch	2019-06-17	6.8	CVE-2018-19450 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	action. An attacker can leverage this to gain remote code execution.			
fusionpbx -- fusionpbx	app/operator_panel/index_inc.php in the Operator Panel module in FusionPBX 4.4.3 suffers from an information disclosure vulnerability due to excessive debug information, which allows authenticated administrative attackers to obtain credentials and other sensitive information.	2019-06-17	4.0	CVE-2019-11407 MISC MISC
fusionpbx -- fusionpbx	XSS in app/operator_panel/index_inc.php in the Operator Panel module in FusionPBX 4.4.3 allows remote unauthenticated attackers to inject arbitrary JavaScript characters by placing a phone call using a specially crafted caller ID number. This can further lead to remote code execution by chaining this vulnerability with a command injection vulnerability also present in FusionPBX.	2019-06-17	4.3	CVE-2019-11408 MISC MISC MISC
fusionpbx -- fusionpbx	app/operator_panel/exec.php in the Operator Panel module in FusionPBX 4.4.3 suffers from a command injection vulnerability due to a lack of input validation that allows authenticated non-administrative attackers to execute commands on the host. This can further lead to remote code execution when combined with an	2019-06-17	6.5	CVE-2019-11409 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	XSS vulnerability also present in the FusionPBX Operator Panel module.			
genieaccess -- wip3bvaf_firmware	Genie Access WIP3BVAF WISH IP 3MP IR Auto Focus Bullet Camera devices through 3.x are vulnerable to directory traversal via the web interface, as demonstrated by reading /etc/shadow. NOTE: this product is discontinued, and its final firmware version has this vulnerability (4.x versions exist only for other Genie Access products).	2019-06-17	5.0	CVE-2019-7315 MISC
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a user with the capability of installing or deleting apps on the device using the web management interface. It seems that the device does not implement any cross-site request forgery protection mechanism which allows an attacker to trick a user who navigates to an attacker controlled page to install or delete an application on the device. Note: The cross-site request forgery is a systemic issue across all other functionalities of the device.	2019-06-17	6.8	CVE-2017-9381 MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite	2019-06-17	4.0	CVE-2017-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "file" as one of the service actions for a normal user to read a file that is stored under the /etc/cmh-lu folder. It retrieves the value from the "parameters" query string variable and then passes it to an internal function "FileUtils::ReadFileIntoBuffer" which is a library function that does not perform any sanitization on the value submitted and this allows an attacker to use directory traversal characters "../" and read files from other folders within the device.			9382 MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "wget" as one of the service actions for a normal user to connect the device to an external website. It retrieves the parameter "URL" from the query string and then passes it to an internal function that uses the curl module on the device to	2019-06-17	6.5	CVE-2017-9383 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	retrieve the contents of the website.			
getvera -- veraedge_firmware	An issue was discovered on Vera Veralite 1.7.481 devices. The device has an additional OpenWRT interface in addition to the standard web interface which allows the highest privileges a user can obtain on the device. This web interface uses root as the username and the password in the /etc/cmh/cmh.conf file which can be extracted by an attacker using a directory traversal attack, and then log in to the device with the highest privileges.	2019-06-17	5.0	CVE-2017-9385 MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a script file called "get_file.sh" which allows a user to retrieve any file stored in the "cmh-ext" folder on the device. However, the "filename" parameter is not validated correctly and this allows an attacker to directory traverse outside the /cmh-ext folder and read any file on the device. It is necessary to create the folder "cmh-ext" on the device which can be executed by an attacker first in an unauthenticated fashion and then execute a directory traversal attack.	2019-06-17	4.0	CVE-2017-9386 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a shell script called connect.sh which is supposed to return a specific cookie for the user when the user is authenticated to https://home.getvera.com. One of the parameters retrieved by this script is "RedirectURL". However, the application lacks strict input validation of this parameter and this allows an attacker to execute the client-side code on this application.	2019-06-17	4.3	CVE-2017-9390 MISC MISC BUGTRAQ
gnu -- bash	A heap-based buffer overflow exists in GNU Bash before 4.3 when wide characters, not supported by the current locale set in the LC_CTYPE environment variable, are printed through the echo built-in function. A local attacker, who can provide data to print through the "echo -e" built-in function, may use this flaw to crash a script or execute code with the privileges of the bash process. This occurs because ansicstr() in lib/sh/strtrans.c mishandles u32cconv().	2019-06-18	4.6	CVE-2012-6711 MISC BID MISC
google -- android	In publishKeyEvent, publishMotionEvent and sendUnchainedFinishedSignal of InputTransport.cpp, there are uninitialized data leading to local information disclosure with no	2019-06-19	4.9	CVE-2019-2004 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-115739809			
google -- android	In onPermissionGrantResult of GrantPermissionsActivity.java, there is a possible incorrectly granted permission due to a missing permission check. This could lead to local escalation of privilege on a locked device with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-68777217	2019-06-19	6.8	CVE-2019-2005 MISC
i-doit -- i-doit	An XSS issue was discovered in i-doit Open 1.12 via the src/tools/php/qr/qr.php url parameter.	2019-06-18	4.3	CVE-2019-6965 MISC
ibm -- campaign	IBM Campaign 9.1.2 and 10.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 162172.	2019-06-19	4.0	CVE-2019-4384 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cloud_private	IBM Cloud Private 2.1.0, 3.1.0, 3.1.1, and 3.1.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 158338.	2019-06-18	6.8	CVE-2019-4142 XF CONFIRM
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 could allow a remote attacker to obtain sensitive information, caused by a flaw in the HTTP OPTIONS method, aka Optionsbleed. By sending an OPTIONS HTTP request, a remote attacker could exploit this vulnerability to read secret data from process memory and obtain sensitive information. IBM X-Force ID: 158878.	2019-06-17	4.0	CVE-2019-4173 CONFIRM XF
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 could allow a remote attacker to bypass security restrictions, caused by an error related to insecure HTTP Methods. An attacker could exploit this vulnerability to gain access to the system. IBM X-Force ID: 158881.	2019-06-17	5.0	CVE-2019-4176 CONFIRM XF
ibm -- infosphere_governance_catalog	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to a XML External Entity Injection (XXE) attack	2019-06-17	5.5	CVE-2018-1845 XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 150905.			CONFIRM
ibm -- marketing_platform	IBM Marketing Platform 9.1.0, 9.1.2, 10.0, and 10.1 exposes sensitive information in the headers that could be used by an authenticated attacker in further attacks against the system. IBM X-Force ID: 120906.	2019-06-19	4.0	CVE-2017-1107 XF CONFIRM
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that any malicious user connecting to the device can change the default SSID and password thereby denying the owner an access to his/her own device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.	2019-06-17	4.0	CVE-2017-10718 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has default Wi-Fi credentials that are exactly the same for every device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.	2019-06-17	4.0	CVE-2017-10719 MISC MISC BUGTRAQ
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wi-Fi name. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too.	2019-06-17	4.6	CVE-2017-10720 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The application uses a dynamic link library(DLL) called "avilib.dll" which is used by the application to send binary packets to the device that allow to control the device. One such action that the DLL provides is change password in the function "sendchangename" which allows a user to change the Wi-Fi name on the device. This function calls a sub function "sub_75876EA0" at address 0x758784F8. The function determines which action to execute based on the parameters sent to it. The "sendchangename" passes the datastring as the second argument which is the name we enter in the textbox and integer 1 as first argument. The rest of the 3 arguments are set to 0. The function "sub_75876EA0" at address 0x75876F19 uses the first argument received and to determine which block to jump to. Since the argument passed is 1, it jumps to 0x75876F20 and proceeds from there to address 0x75876F56 which calculates the length of the data string passed as the first parameter. This length and the first argument are then passed to the address 0x75877001 which calls the memmove function which uses a stack address as the destination where the password typed by us is passed as the source and length calculated above is passed as the number of bytes to			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	copy which leads to a stack overflow.			
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has Telnet functionality enabled by default. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.	2019-06-17	4.0	CVE-2017-10721 MISC MISC BUGTRAQ
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wi-Fi password. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an	2019-06-17	4.6	CVE-2017-10722 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to get access to all the data that the user has access too. The application uses a dynamic link library(DLL) called "avilib.dll" which is used by the application to send binary packets to the device that allow to control the device. One such action that the DLL provides is change password in the function "sendchangepass" which allows a user to change the Wi-Fi password on the device. This function calls a sub function "sub_75876EA0" at address 0x7587857C. The function determines which action to execute based on the parameters sent to it. The "sendchangepass" passes the datastring as the second argument which is the password we enter in the textbox and integer 2 as first argument. The rest of the 3 arguments are set to 0. The function "sub_75876EA0" at address 0x75876F19 uses the first argument received and to determine which block to jump to. Since the argument passed is 2, it jumps to 0x7587718C and proceeds from there to address 0x758771C2 which calculates the length of the data string passed as the first parameter.This length and the first argument are then passed to the address 0x7587726F which calls a memmove function which uses a stack address as the destination where the password typed by us is passed as the source			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and length calculated above is passed as the number of bytes to copy which leads to a stack overflow.			
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device Wi-Fi SSID can exploit a memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries. The firmware contains binary uvc_stream that is the UDP daemon which is responsible for handling all the UDP requests that the device receives. The client application sends a UDP request to change the Wi-Fi name which contains the following format: "SETCMD0001+0001+[2 byte length of wifiname]+[Wifiname].	2019-06-17	6.5	CVE-2017-10723 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This request is handled by "control_Dev_thread" function which at address "0x00409AE0" compares the incoming request and determines if the 10th byte is 01 and if it is then it redirects to 0x0040A74C which calls the function "setwifiname". The function "setwifiname" uses a memcpy function but uses the length of the payload obtained by using strlen function as the third parameter which is the number of bytes to copy and this allows an attacker to overflow the function and control the $PC value.			
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device Wi-Fi SSID can exploit a memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of	2019-06-17	6.5	CVE-2017-10724 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	nation critical infrastructure/industries. The firmware contains binary uvc_stream that is the UDP daemon which is responsible for handling all the UDP requests that the device receives. The client application sends a UDP request to change the Wi-Fi name which contains the following format: "SETCMD0001+0002+[2 byte length of wifipassword]+[Wifipassword]. This request is handled by "control_Dev_thread" function which at address "0x00409AE4" compares the incoming request and determines if the 10th byte is 02 and if it is then it redirects to 0x0040A7D8, which calls the function "setwifipassword". The function "setwifipassword" uses a memcpy function but uses the length of the payload obtained by using strlen function as the third parameter which is the number of bytes to copy and this allows an attacker to overflow the function and control the $PC value.			
jspxcms -- jspxcms	In Jspxcms 9.0.0, a vulnerable URL routing implementation allows remote code execution after logging in as web admin.	2019-06-20	6.5	CVE-2018-16553 MISC MISC
kcodes -- netusb.ko	An exploitable arbitrary memory read vulnerability exists in the	2019-06-17	6.4	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	KCodes NetUSB.ko kernel module which enables the ReadySHARE Printer functionality of at least two NETGEAR Nighthawk Routers and potentially several other vendors/products. A specially crafted index value can cause an invalid memory read, resulting in a denial of service or remote information disclosure. An unauthenticated attacker can send a crafted packet on the local network to trigger this vulnerability.			5016 BID MISC
kcodes -- netusb.ko	An exploitable information disclosure vulnerability exists in the KCodes NetUSB.ko kernel module that enables the ReadySHARE Printer functionality of at least two NETGEAR Nighthawk Routers and potentially several other vendors/products. An unauthenticated, remote attacker can craft and send a packet containing an opcode that will trigger the kernel module to return several addresses. One of which can be used to calculate the dynamic base address of the module for further exploitation.	2019-06-17	5.0	CVE-2019-5017 BID MISC
linksys -- wrt1900acs_firmware	An issue was discovered on Linksys WRT1900ACS 1.0.3.187766 devices. An ability exists for an unauthenticated user	2019-06-17	5.0	CVE-2019-7579

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to browse a confidential ui/1.0.99.187766/dynamic/js/setup.js.localized file on the router's webserver, allowing for an attacker to identify possible passwords that the system uses to set the default guest network password. An attacker can use this list of 30 words along with a random 2 digit number to brute force their access onto a router's guest network.			MISC MISC
linux -- linux_kernel	i915_gem_userptr_get_pages in drivers/gpu/drm/i915/i915_gem_userptr.c in the Linux kernel 4.15.0 on Ubuntu 18.04.2 allows local users to cause a denial of service (NULL pointer dereference and BUG) or possibly have unspecified other impact via crafted ioctl calls to /dev/dri/card0.	2019-06-18	4.6	CVE-2019-12881 MISC
misp -- misp	app/Model/Server.php in MISP 2.4.109 allows remote command execution by a super administrator because the PHP file_exists function is used with user-controlled entries, and phar:// URLs trigger deserialization.	2019-06-17	6.5	CVE-2019-12868 MISC
my-netdata -- netdata	An issue was discovered in Netdata 1.10.0. JSON injection exists via the api/v1/data tqx parameter because of web_client_api_request_v1_data in web/api/web_api_v1.c.	2019-06-18	4.3	CVE-2018-18836 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM MISC
my-netdata -- netdata	An issue was discovered in Netdata 1.10.0. HTTP Header Injection exists via the api/v1/data filename parameter because of web_client_api_request_v1_data in web/api/web_api_v1.c.	2019-06-18	5.8	CVE-2018-18837 MISC MISC CONFIRM MISC
my-netdata -- netdata	An issue was discovered in Netdata 1.10.0. Log Injection (or Log Forgery) exists via a %0a sequence in the url parameter to api/v1/registry.	2019-06-18	5.0	CVE-2018-18838 MISC CONFIRM MISC
my-netdata -- netdata	** DISPUTED ** An issue was discovered in Netdata 1.10.0. Full Path Disclosure (FPD) exists via api/v1/alarms. NOTE: the vendor says "is intentional."	2019-06-18	5.0	CVE-2018-18839 MISC MISC MISC
nagios -- nagios_xi	An Insufficient Access Control vulnerability (leading to credential disclosure) in coreconfigsnapshot.php (aka configuration snapshot page) in Nagios XI before 5.5.4 allows remote attackers to gain access to	2019-06-19	5.0	CVE-2018-17148 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configuration files containing confidential credentials.			
ngahr -- resourcelink	NGA ResourceLink 20.0.2.1 allows local file inclusion.	2019-06-19	4.0	CVE-2018-18863 MISC
open-xchange -- open-xchange_appsuite	OX App Suite 7.10.1 and earlier allows Information Exposure.	2019-06-18	5.0	CVE-2019-7159 MISC MISC
openfind -- mail2000	An issue was discovered in Openfind Mail2000 v6 Webmail. XSS can occur via an '<object data="data:text/html' substring in an e-mail message (The vendor subsequently patched this).	2019-06-19	4.3	CVE-2019-9763 MISC
otrs -- otrs	An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.8, Community Edition 6.0.x through 6.0.19, and Community Edition 5.0.x through 5.0.36. In the customer or external frontend, personal information of agents (e.g., Name and mail address) can be disclosed in external notes.	2019-06-17	5.0	CVE-2019-12497 MISC CONFIRM
php -- php	When using gdImageCreateFromXbm() function of PHP gd extension in PHP versions 7.1.x below 7.1.30,	2019-06-18	5.0	CVE-2019-11038

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	7.2.x below 7.2.19 and 7.3.x below 7.3.6, it is possible to supply data that will cause the function to use the value of uninitialized variable. This may lead to disclosing contents of the stack that has been left there by previous code.			CONFIRM
php -- php	Function iconv_mime_decode_headers() in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 may perform out-of-buffer read due to integer overflow when parsing MIME headers. This may lead to information disclosure or crash.	2019-06-18	6.4	CVE-2019-11039 CONFIRM
php -- php	When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.	2019-06-18	6.4	CVE-2019-11040 CONFIRM
radare -- radare2	In radare2 through 3.5.1, cmd_mount in libr/core/cmd_mount.c has a double free for the ms command.	2019-06-17	4.3	CVE-2019-12865 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ranksol -- live_call_support	CSRF exists in server.php in Live Call Support Application 1.5 for adding an admin account.	2019-06-19	6.8	CVE-2018-17389 MISC MISC
ranksol -- nimble_professional	CSRF exists in Nimble Messaging Bulk SMS Marketing Application 1.0 for adding an admin account.	2019-06-19	6.8	CVE-2018-17387 MISC MISC
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Since Gem::UserInteraction#verbose calls say without escaping, escape sequence injection is possible.	2019-06-17	5.0	CVE-2019-8321 MISC
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. The gem owner command outputs the contents of the API response directly to stdout. Therefore, if the response is crafted, escape sequence injection may occur.	2019-06-17	5.0	CVE-2019-8322 MISC
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Gem::GemcutterUtilities#with_response may output the API response to stdout as it is. Therefore, if the API side modifies	2019-06-17	5.0	CVE-2019-8323 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the response, escape sequence injection may occur.			
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. A crafted gem with a multi-line name is not handled correctly. Therefore, an attacker could inject arbitrary code to the stub line of gemspec, which is eval-ed by code in ensure_loadable_spec during the preinstall check.	2019-06-17	6.8	CVE-2019-8324 MISC
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Since Gem::CommandManager#run calls alert_error without escaping, escape sequence injection is possible. (There are many ways to cause an error.)	2019-06-17	5.0	CVE-2019-8325 MISC
sahipro -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7.x.x and 8.0.0. A web reports module has "export to excel features" that are vulnerable to CSV injection. An attacker can embed Excel formulas inside an automation script that, when exported after execution, results in code execution.	2019-06-17	6.8	CVE-2018-20468 MISC
sahipro -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7.x.x and 8.0.0. The logs web interface is vulnerable to stored XSS.	2019-06-17	4.3	CVE-2018-20472

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
samba -- samba	Samba 4.9.x before 4.9.9 and 4.10.x before 4.10.5 has a NULL pointer dereference, leading to Denial of Service. This is related to the AD DC DNS management server (dnsserver) RPC server process.	2019-06-19	4.0	CVE-2019-12435 BID UBUNTU CONFIRM
samba -- samba	Samba 4.10.x before 4.10.5 has a NULL pointer dereference, leading to an AD DC LDAP server Denial of Service. This is related to an attacker using the paged search control. The attacker must have directory read access in order to attempt an exploit.	2019-06-19	4.0	CVE-2019-12436 BID UBUNTU CONFIRM
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of setting a name for the wireless network. These values are stored by the device in NVRAM (Non-volatile RAM). It seems that the POST parameters passed in this request to set up names on the device do not have a string length check on them. This allows an attacker to send a large payload in the "mssid_1" POST parameter. The device also allows a user to	2019-06-18	4.6	CVE-2017-8329 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	view the name of the Wifi Network set by the user. While processing this request, the device calls a function at address 0x00412CE4 (routerSummary) in the binary "webServer" located in Almond folder, which retrieves the value set earlier by "mssid_1" parameter as SSID2 and this value then results in overflowing the stack set up for this function and allows an attacker to control $ra register value on the stack which allows an attacker to control the device by executing a payload of an attacker's choice. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST parameter "mssid_1" at address 0x0042BA00 and then sets in the NVRAM at address 0x0042C314. The value is later retrieved in the function at address 0x00412EAC and this results in overflowing the buffer as the function copies the value directly on the stack.			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of adding new port forwarding rules to the device. It seems that the POST parameters passed in this request to set up routes on the device can be set in such a way that would result in passing commands to a "system" API in the function and thus result in command injection on the device. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that recieves the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function sub_43C280in IDA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "ip_address" is extracted at address 0x0043C2F0. The POST parameter "ipaddress" is concatenated at address 0x0043C958 and this is passed to a "system" function at address 0x00437284. This allows an attacker to provide the payload of	2019-06-18	6.5	CVE-2017-8331 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	his/her choice and finally take control of the device.			
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of blocking key words passing in the web traffic to prevent kids from watching content that might be deemed unsafe using the web management interface. It seems that the device does not implement any cross-site scripting protection mechanism which allows an attacker to trick a user who is logged in to the web management interface into executing a stored cross-site scripting payload on the user's browser and execute any action on the device provided by the web management interface.	2019-06-18	6.5	CVE-2017-8332 MISC MISC BUGTRAQ
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of blocking IP addresses using the web management interface. It seems that the device does not implement any cross-site scripting forgery protection mechanism which allows an attacker to trick a user who is logged in to the web management interface into executing a cross-site scripting	2019-06-18	6.0	CVE-2017-8334 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	payload on the user's browser and execute any action on the device provided by the web management interface.			
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of setting name for wireless network. These values are stored by the device in NVRAM (Non-volatile RAM). It seems that the POST parameters passed in this request to set up names on the device do not have a string length check on them. This allows an attacker to send a large payload in the "mssid_1" POST parameter. The device also allows a user to view the name of the Wifi Network set by the user. While processing this request, the device calls a function named "getCfgToHTML" at address 0x004268A8 which retrieves the value set earlier by "mssid_1" parameter as SSID2 and this value then results in overflowing the stack set up for this function and allows an attacker to control $ra register value on the stack which allows an attacker to control the device by executing a payload of an attacker's choice. If the firmware version AL-R096 is dissected using binwalk tool, we	2019-06-18	6.0	CVE-2017-8335 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that recieves the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST parameter "mssid_1" at address 0x0042BA00 and then sets in the NVRAM at address 0x0042C314. The value is later retrieved in the function "getCfgToHTML" at address 0x00426924 and this results in overflowing the buffer due to "strcat" function that is utilized by this function.			
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of adding new routes to the device. It seems that the POST parameters passed in this request to set up routes on the device can be set in such a way that would result in overflowing the stack set up and allow an attacker to control the $ra register stored on the stack. If the firmware version AL-R096 is dissected using binwalk tool, we	2019-06-18	6.5	CVE-2017-8336 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that recieves the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST request. The POST parameter "gateway" allows to overflow the stack and control the $ra register after 1546 characters. The value from this post parameter is then copied on the stack at address 0x00421348 as shown below. This allows an attacker to provide the payload of his/her choice and finally take control of the device.			
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of executing various actions on the web management interface. It seems that the device does not implement any Origin header check which allows an attacker who can trick a user to navigate to an attacker's webpage to exploit this issue and brute force the password for the web management	2019-06-18	6.8	CVE-2017-8337 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	interface. It also allows an attacker to then execute any other actions which include management if rules, sensors attached to the devices using the websocket requests.			
seeddms -- seeddms	SeedDMS before 5.1.11 allows Remote Command Execution (RCE) because of unvalidated file upload of PHP scripts, a different vulnerability than CVE-2018-12940.	2019-06-20	6.0	CVE-2019-12744 MISC CONFIRM
seeddms -- seeddms	out/out.GroupMgr.php in SeedDMS 5.1.11 has Stored XSS by making a new group with a JavaScript payload as the "GROUP" Name.	2019-06-17	4.3	CVE-2019-12801 MISC
teltonika -- rut950_firmware	An issue was discovered on Teltonika RTU950 R_31.04.89 devices. The application allows a user to login without limitation. For every successful login request, the application saves a session. A user can re-login without logging out, causing the application to store the session in memory. Exploitation of this vulnerability will increase memory use and consume free space.	2019-06-19	6.8	CVE-2018-19878 MISC MISC
tp-link -- tl-wr1043nd_firmware	An issue was discovered on TP-Link TL-WR1043ND V2 devices. The credentials can be easily	2019-06-19	5.0	CVE-2019-6972

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	decoded and cracked by brute-force, WordList, or Rainbow Table attacks. Specifically, credentials in the "Authorization" cookie are encoded with URL encoding and base64, leading to easy decoding. Also, the username is cleartext, and the password is hashed with the MD5 algorithm (after decoding of the URL encoded string with base64).			MISC MISC
tubigan -- welcome_to_our_resort	The Tubigan "Welcome to our Resort" 1.0 software allows CSRF via admin/mod_users/controller.php?action=edit.	2019-06-18	6.8	CVE-2018-18802 MISC MISC
twistedmatrix -- twisted	In words.protocols.jabber.xmlstream in Twisted through 19.2.1, XMPP support did not verify certificates when used with TLS, allowing an attacker to MITM connections.	2019-06-16	5.8	CVE-2019-12855 MISC MISC
urbackup -- urbackup	In UrBackup 2.2.6, an attacker can send a malformed request to the client over the network, and trigger a fileservplugin/CClientThread.cpp CClientThread::ProcessPacket metadata_id!=0 assertion, leading to shutting down the client application.	2019-06-18	5.0	CVE-2018-20013 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
znc -- znc	Modules.cpp in ZNC before 1.7.4-rc1 allows remote authenticated non-admin users to escalate privileges and execute arbitrary code by loading a module with a crafted name.	2019-06-15	6.5	CVE-2019-12816 CONFIRM CONFIRM MLIST BUGTRAQ
zrlog -- zrlog	An issue was discovered in ZRLOG 2.0.1. There is a Stored XSS vulnerability in the nickname field of the comment area.	2019-06-19	4.3	CVE-2018-17079 MISC MISC
zucchetti -- hr_portal	Zucchetti HR Portal through 2019-03-15 allows Directory Traversal. Unauthenticated users can escape outside of the restricted location (dot-dot-slash notation) to access files or directories that are elsewhere on the system. Through this vulnerability it is possible to read the application's java sources from /WEB-INF/classes/*.class	2019-06-19	5.0	CVE-2019-10257 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
b3log -- symphony	In Symphony before 3.3.0, there is XSS in the Title under Post. The ID "articleTitle" of this is stored in the "articleTitle" JSON field, and executes a payload when accessing the /member/test/points URI, allowing remote attacks. Any Web script or HTML can be inserted by an admin-authenticated user via a crafted web site name.	2019-06-20	3.5	CVE-2018-16249 MISC
cisco -- prime_service_catalog	A vulnerability in the web-based management interface of Cisco Prime Service Catalog could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by adding specific strings to multiple configuration fields. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.	2019-06-19	3.5	CVE-2019-1875 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, a stored Cross-site scripting (XSS) vulnerability allows remote authenticated users to inject arbitrary web script via changestationname.php.	2019-06-18	3.5	CVE-2018-18875 MISC MISC
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, a networkdiags.php reflected Cross-site scripting (XSS) vulnerability allows remote authenticated users to inject arbitrary web script.	2019-06-18	3.5	CVE-2018-18880 MISC MISC
concrete5 -- concrete5	Concrete5 8.4.3 has XSS because config/concrete.php allows uploads (by administrators) of SVG files that may contain HTML data with a SCRIPT element.	2019-06-17	3.5	CVE-2018-19146 MISC MISC MISC MISC
creatiwity -- witycms	The "utilisateur" menu in Creatiwity wityCMS 0.6.2 modifies the presence of XSS at two input points for user information, with the "first name" and "last name" parameters.	2019-06-20	3.5	CVE-2018-16250 MISC
e107 -- e107	An issue was discovered in e107 v2.1.9. There is a XSS	2019-06-19	3.5	CVE-2018-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attack on e107_admin/comment.php.			17423 MISC MISC
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a shell script called relay.sh which is used for creating new SSH relays for the device so that the device connects to Vera servers. All the parameters passed in this specific script are logged to a log file called log.relay in the /tmp folder. The user can also read all the log files from the device using a script called log.sh. However, when the script loads the log files it displays them with content-type text/html and passes all the logs through the ansi2html binary which converts all the character text including HTML meta-characters correctly to be displayed in the browser. This allows an attacker to use the log files as a storing mechanism for the XSS payload and thus whenever a user navigates to that log.sh script, it enables the XSS payload and allows an attacker to execute his malicious payload on the user's browser.	2019-06-17	3.5	CVE-2017-9387 MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158332.	2019-06-17	3.5	CVE-2019-4136 CONFIRM XF
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 158879.	2019-06-17	2.1	CVE-2019-4174 CONFIRM XF
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 158882.	2019-06-17	2.1	CVE-2019-4177 CONFIRM XF
ibm -- control_desk	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	2019-06-19	3.5	CVE-2019-4303 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949.			
ibm -- i	IBM i 7.27.3 Clustering could allow a local attacker to obtain sensitive information, caused by the use of advanced node failure detection using the REST API to interface with the HMC. An attacker could exploit this vulnerability to obtain HMC credentials. IBM X-Force ID: 162159.	2019-06-14	2.1	CVE-2019-4381 BID XF CONFIRM
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the View Filters page (view_filters_page.php) and Edit Filter page (manage_filter_edit_page.php) in MantisBT 2.1.0 through 2.17.0 allows remote attackers to inject arbitrary code (if CSP settings permit it) through a crafted PATH_INFO. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-13055.	2019-06-20	2.6	CVE-2018-16514 MISC
microfocus -- fortify_software_security_center	Cross-Site Scripting vulnerability in Micro Focus Fortify Software Security Center Server, versions 17.2, 18.1, 18.2, has been identified	2019-06-19	3.5	CVE-2019-11649 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in Micro Focus Software Security Center. The vulnerability could be exploited to execute JavaScript code in user?s browser. The vulnerability could be exploited to execute JavaScript code in user?s browser.			
nagios -- nagios_xi	A cross-site scripting vulnerability exists in Nagios XI before 5.5.4 via the 'name' parameter within the Account Information page. Exploitation of this vulnerability allows an attacker to execute arbitrary JavaScript code within the auto login admin management page.	2019-06-19	3.5	CVE-2018-17146 MISC
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a UPnP functionality for devices to interface with the router and interact with the device. It seems that the "NewInMessage" SOAP parameter passed with a huge payload results in crashing the process. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all	2019-06-18	3.3	CVE-2017-8330 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the binaries. The binary "miniupnpd" is the one that has the vulnerable function that receives the values sent by the SOAP request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function WscDevPutMessage at address 0x0041DBB8 in IDA pro is identified to be receiving the values sent in the SOAP request. The SOAP parameter "NewInMesage" received at address 0x0041DC30 causes the miniupnpd process to finally crash when a second request is sent to the same process.			
seeddms -- seeddms	out/out.UsrMgr.php in SeedDMS before 5.1.11 allows Stored Cross-Site Scripting (XSS) via the name field.	2019-06-20	3.5	CVE-2019-12745 MISC CONFIRM
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCtl 0x8000204B.	2019-06-21	2.1	CVE-2018-15729 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCtl 0x80002067.	2019-06-21	2.1	CVE-2018-15730 MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCtl 0x8000205B.	2019-06-21	2.1	CVE-2018-15731 MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCtl 0x80002063.	2019-06-21	2.1	CVE-2018-15732 MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a NULL Pointer Dereference vulnerability due to not validating the size of the output buffer value from IOCtl 0x80002028.	2019-06-21	2.1	CVE-2018-15733 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCtl 0x8000206B.	2019-06-21	2.1	CVE-2018-15734 MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCtl 0x8000206F.	2019-06-21	2.1	CVE-2018-15735 MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCtl 0x8000204F.	2019-06-21	2.1	CVE-2018-15736 MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCtl 0x80002043.	2019-06-21	2.1	CVE-2018-15737 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
symantec -- data_loss_prevention	DLP 15.5 MP1 and all prior versions may be susceptible to a cross-site scripting (XSS) vulnerability, a type of issue that can enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.	2019-06-19	3.5	CVE-2019-9701 MISC
yzmcms -- yzmcms	YzmCMS 5.1 has XSS via the admin/system_manage/user_config_add.html title parameter.	2019-06-20	3.5	CVE-2018-16247 MISC

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
akamai -- cloudtest	Akamai CloudTest before 58.30 allows remote code execution.	2019-06-21	not yet calculated	CVE-2019-11011 CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NFIRM
apache -- geode	When an Apache Geode server versions 1.0.0 to 1.8.0 is operating in secure mode, a user with write permissions for specific data regions can modify internal cluster metadata. A malicious user could modify this data in a way that affects the operation of the cluster.	2019-06-21	not yet calculated	CVE-2017-15694 MISC
apache -- tomcat	The fix for CVE-2019-0199 was incomplete and did not address HTTP/2 connection window exhaustion on write in Apache Tomcat versions 9.0.0.M1 to 9.0.19 and 8.5.0 to 8.5.40 . By not sending WINDOW_UPDATE messages for the connection window (stream 0) clients were able to cause server-side threads to block eventually leading to thread exhaustion and a DoS.	2019-06-21	not yet calculated	CVE-2019-10072 MISC
asus -- vivobaby_for_android	The ASUS Vivobaby application before 1.1.09 for Android has Missing SSL Certificate Validation.	2019-06-20	not yet calculated	CVE-2017-17944 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
axentra -- hipserv	/api/2.0/rest/aggregator/xml in Axentra firmware, used by NETGEAR Stora, Seagate GoFlex Home, and MEDION LifeCloud, has an XXE vulnerability that can be chained with an SSRF bug to gain remote command execution as root. It can be triggered by anyone who knows the IP address of the affected device.	2019-06-19	not yet calculated	CVE-2018-18471 MISC MISC
bobronix -- jeditor_for_jira	The Bobronix JEditor editor before 3.0.6 for Jira allows an attacker to add a URL/Link (to an existing issue) that can cause forgery of a request to an out-of-origin domain. This in turn may allow for a forged request that can be invoked in the context of an authenticated user, leading to stealing of session tokens and account takeover.	2019-06-21	not yet calculated	CVE-2019-12836 MISC CONFIRM
cerio -- dt-300n_devices	Cerio DT-300N 1.1.6 through 1.1.12 devices allow OS command injection because of improper input validation of the web-interface PING feature's use of Save.cgi to execute a ping command, as exploited in the wild in October 2018.	2019-06-18	not yet calculated	CVE-2018-18852 MISC
check_point_software_technologies --	Check Point Endpoint Security Client for Windows, with Anti-	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
endpoint_security_client_for_windows	Malware blade installed, before version E81.00, tries to load a non-existent DLL during an update initiated by the UI. An attacker with administrator privileges can leverage this to gain code execution within a Check Point Software Technologies signed binary, where under certain circumstances may cause the client to terminate.	06-20	calculated	2019-8458 CONFIRM
check_point_software_technologies -- endpoint_security_client_for_windows	Check Point Endpoint Security Client for Windows, with the VPN blade, before version E80.83, starts a process without using quotes in the path. This can cause loading of a previously placed executable with a name similar to the parts of the path, instead of the intended one.	2019-06-20	not yet calculated	CVE-2019-8459 CONFIRM
cisco -- rv110w_and_rv130w_and_rv215w_routers	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to disconnect clients that are connected to the guest network on an affected router. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for device disconnection and providing the connected device	2019-06-19	not yet calculated	CVE-2019-1897 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	information. A successful exploit could allow the attacker to deny service to specific clients that are connected to the guest network.			
cisco -- rv110w_and_rv130w_and_rv215w_routers	A vulnerability in the web interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to acquire the list of devices that are connected to the guest network. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing a specific URI on the web interface of the router.	2019-06-19	not yet calculated	CVE-2019-1899 BID CISCO
cisco -- rv110w_and_rv130w_and_rv215w_routers	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to access the syslog file on an affected device. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for the syslog file. A successful exploit could allow the attacker to access the information contained in the file.	2019-06-19	not yet calculated	CVE-2019-1898 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- staros	A vulnerability in the internal packet-processing functionality of the Cisco StarOS operating system running on virtual platforms could allow an unauthenticated, remote attacker to cause an affected device to stop processing traffic, resulting in a denial of service (DoS) condition. The vulnerability is due to a logic error that may occur under specific traffic conditions. An attacker could exploit this vulnerability by sending a series of crafted packets to an affected device. A successful exploit could allow the attacker to prevent the targeted service interface from receiving any traffic, which would lead to a DoS condition on the affected interface. The device may have to be manually reloaded to recover from exploitation of this vulnerability.	2019-06-19	not yet calculated	CVE-2019-1869 BID CISCO
cisco -- dna_center	A vulnerability in Cisco Digital Network Architecture (DNA) Center could allow an unauthenticated, adjacent attacker to bypass authentication and access critical internal services. The vulnerability is due to insufficient access restriction to ports necessary for system operation. An attacker could exploit this vulnerability by	2019-06-19	not yet calculated	CVE-2019-1848 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	connecting an unauthorized network device to the subnet designated for cluster services. A successful exploit could allow an attacker to reach internal services that are not hardened for external access.			
cisco -- email_security_appliance	A vulnerability in the GZIP decompression engine of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured content filters on the device. The vulnerability is due to improper validation of GZIP-formatted files. An attacker could exploit this vulnerability by sending a malicious file inside a crafted GZIP-compressed file. A successful exploit could allow the attacker to bypass configured content filters that would normally drop the email.	2019-06-19	not yet calculated	CVE-2019-1905 BID CISCO
cisco -- integrated_management_controller	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF	2019-06-19	not yet calculated	CVE-2019-1632 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	protections for the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user to follow a malicious link. A successful exploit could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on the affected device.			
cisco -- integrated_management_controller	A vulnerability in the CLI of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient validation of user-supplied input at the CLI. An attacker could exploit this vulnerability by authenticating with the administrator password via the CLI of an affected device and submitting crafted input to the affected commands. A successful exploit could allow the attacker to execute arbitrary commands on the device with root privileges.	2019-06-19	not yet calculated	CVE-2019-1879 BID CISCO
cisco -- integrated_management_controller	A vulnerability in the Server Utilities of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to gain	2019-06-19	not yet calculated	CVE-2019-162

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthorized access to sensitive user information from the configuration data that is stored on the affected system. The vulnerability is due to insufficient protection of data in the configuration file. An attacker could exploit this vulnerability by downloading the configuration file. An exploit could allow the attacker to use the sensitive information from the file to elevate privileges.			7 BID CISCO
cisco -- integrated_management_controller	A vulnerability in the firmware signature checking program of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient checking of an input buffer. An attacker could exploit this vulnerability by passing a crafted file to the affected system. A successful exploit could inhibit an administrator's ability to access the system.	2019-06-19	not yet calculated	CVE-2019-1630 BID CISCO
cisco -- integrated_management_controller	A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting	2019-06-19	not yet calculated	CVE-2019-162

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in a denial of service (DoS) condition on an affected device. The vulnerability is due to incorrect bounds checking. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected system. An exploit could allow the attacker to cause a buffer overflow, resulting in a process crash and DoS condition on the device.			8 BID CISCO
cisco -- integrated_management_controller	A vulnerability in the configuration import utility of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to have write access and upload arbitrary data to the filesystem. The vulnerability is due to a failure to delete temporarily uploaded files. An attacker could exploit this vulnerability by crafting a malicious file and uploading it to the affected device. An exploit could allow the attacker to fill up the filesystem or upload malicious scripts.	2019-06-19	not yet calculated	CVE-2019-1629 BID CISCO
cisco -- ios_xe_software	A vulnerability in the web-based UI (web UI) of Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an	2019-06-20	not yet calculated	CVE-2019-1904

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	affected system. The vulnerability is due to insufficient CSRF protections for the web UI on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or reload an affected device. This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS XE Software with the HTTP Server feature enabled. The default state of the HTTP Server feature is version dependent.			MISC
cisco -- multiple_products	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of user-	2019-06-19	not yet calculated	CVE-2019-1843 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to reload the device and causing a DoS condition.			
cisco -- prime_infrastructure	A vulnerability in the Virtual Domain system of Cisco Prime Infrastructure (PI) could allow an authenticated, remote attacker to change the virtual domain configuration, which could lead to privilege escalation. The vulnerability is due to improper validation of API requests. An attacker could exploit this vulnerability by manipulating requests sent to an affected PI server. A successful exploit could allow the attacker to change the virtual domain configuration and possibly elevate privileges.	2019-06-19	not yet calculated	CVE-2019-1906 BID CISCO
cisco -- sd_wan_solution	A vulnerability in the vManage web-based UI (Web UI) of the Cisco SD-WAN Solution could allow an authenticated, remote attacker to gain elevated privileges on an affected vManage device. The vulnerability is due to a failure to properly authorize certain user actions in the device	2019-06-19	not yet calculated	CVE-2019-1626 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configuration. An attacker could exploit this vulnerability by logging in to the vManage Web UI and sending crafted HTTP requests to vManage. A successful exploit could allow attackers to gain elevated privileges and make changes to the configuration that they would not normally be authorized to make.			
cisco -- sd_wan_solution	A vulnerability in the CLI of Cisco SD-WAN Solution could allow an authenticated, local attacker to elevate lower-level privileges to the root user on an affected device. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by authenticating to the targeted device and executing commands that could lead to elevated privileges. A successful exploit could allow the attacker to make configuration changes to the system as the root user.	2019-06-19	not yet calculated	CVE-2019-1625 BID CISCO
cisco -- sd_wan_solution	A vulnerability in the vManage web-based UI (Web UI) in the Cisco SD-WAN Solution could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input	2019-06-19	not yet calculated	CVE-2019-1624 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the vManage Web UI. A successful exploit could allow the attacker to execute commands with root privileges.			CISCO
cisco -- security_manager	A vulnerability in Cisco Security Manager could allow an unauthenticated, remote attacker to access sensitive information or cause a denial of service (DoS) condition. The vulnerability is due to improper restrictions on XML entities. An attacker could exploit this vulnerability by sending malicious requests to a targeted system that contain references within XML entities. An exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the application to consume available resources, resulting in a DoS condition.	2019-06-19	not yet calculated	CVE-2019-1903 BID CISCO
cisco -- telepresence_codec_and_collaboration_endpoint_software	A vulnerability in the Cisco Discovery Protocol (CDP) implementation for the Cisco TelePresence Codec (TC) and Collaboration Endpoint (CE) Software could allow an unauthenticated, adjacent attacker	2019-06-19	not yet calculated	CVE-2019-1878

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to inject arbitrary shell commands that are executed by the device. The vulnerability is due to insufficient input validation of received CDP packets. An attacker could exploit this vulnerability by sending crafted CDP packets to an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts on the targeted device.			CISCO
cisco -- wide_area_application_services_software	A vulnerability in the HTTPS proxy feature of Cisco Wide Area Application Services (WAAS) Software could allow an unauthenticated, remote attacker to use the Central Manager as an HTTPS proxy. The vulnerability is due to insufficient authentication of proxy connection requests. An attacker could exploit this vulnerability by sending a malicious HTTPS CONNECT message to the Central Manager. A successful exploit could allow the attacker to access public internet resources that would normally be blocked by corporate policies.	2019-06-19	not yet calculated	CVE-2019-1876 BID CISCO
cloud_foundry_foundation -- bosh	Cloud Foundry BOSH 270.x versions prior to v270.1.1, contain a BOSH Director that does not properly redact credentials when	2019-06-18	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configured to use a MySQL database. A local authenticated malicious user may read any credentials that are contained in a BOSH manifest.		ulated	11271 CONFIRM
cloud_foundry_foundation -- uua_release	Cloud Foundry UAA, versions prior to 73.0.0, falls back to appending ?unknown.org? to a user's email address when one is not provided and the user name does not contain an @ character. This domain is held by a private company, which leads to attack vectors including password recovery emails sent to a potentially fraudulent address. This would allow the attacker to gain complete control of the user's account.	2019-06-19	not yet calculated	CVE-2019-3787 CONFIRM
cloudera -- manager	An issue was discovered in Cloudera Manager 5.x through 5.15.0. One type of page in Cloudera Manager uses a 'returnUrl' parameter to redirect the user to another page in Cloudera Manager once a wizard is completed. The validity of this parameter was not checked. As a result, the user could be automatically redirected to an attacker's external site or perform a malicious JavaScript function that results in cross-site scripting (XSS). This was fixed by not	2019-06-20	not yet calculated	CVE-2018-15913 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allowing any value in the returnUrl parameter with patterns such as http://, https://, //, or javascript. The only exceptions to this rule are the SAML Login/Logout URLs, which remain supported since they are explicitly configured and they are not passed via the returnUrl parameter.			
dell_emc -- avamar_adme_web_interface	Dell EMC Avamar ADMe Web Interface 1.0.50 and 1.0.51 are affected by an LFI vulnerability which may allow a malicious user to download arbitrary files from the affected system by sending a specially crafted request to the Web Interface application.	2019-06-19	not yet calculated	CVE-2019-3737 MISC
dell_emc -- supportassist_for_business_and_supportassist_for_home_pcs	Dell SupportAssist for Business PCs version 2.0 and Dell SupportAssist for Home PCs version 2.2, 2.2.1, 2.2.2, 2.2.3, 3.0, 3.0.1, 3.0.2, 3.1, 3.2, and 3.2.1 contain an Improper Privilege Management Vulnerability. A malicious local user can exploit this vulnerability by inheriting a system thread using a leaked thread handle to gain system privileges on the affected machine.	2019-06-20	not yet calculated	CVE-2019-3735 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ethereum -- primeo_token	The doAirdrop function of a smart contract implementation for Primeo (PEO), an Ethereum token, does not check the numerical relationship between the amount of the air drop and the token's total supply, which lets the owner of the contract issue an arbitrary amount of currency. (Increasing the total supply by using 'doAirdrop' ignores the hard cap written in the contract and devalues the token.)	2019-06-19	not yet calculated	CVE-2018-18425 MISC MISC
evernote_corporation -- evernote	A universal Cross-site scripting (UXSS) vulnerability in the Evernote Web Clipper extension before 7.11.1 for Chrome allows remote attackers to run arbitrary web script or HTML in the context of any loaded 3rd-party IFrame.	2019-06-18	not yet calculated	CVE-2019-12592 MISC MISC
excellent_infotec_corporation -- biyan	EXCELLENT INFOTEK BiYan v1.57 ~ v2.8 allows an attacker to leak user information without being authenticated, by sending a LOGIN_ID element to the auth/main/asp/check_user_login_info.aspx URI, and then reading the response, as demonstrated by the KW_EMAIL or KW_TEL field.	2019-06-19	not yet calculated	CVE-2019-11233 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
excellent_infotec_corporation -- biyan	EXCELLENT INFOTEK BiYan v1.57 ~ v2.8 allows an attacker to leak user information (Password) without being authenticated, by sending an EMP_NO element to the kws_login/asp/query_user.asp URI, and then reading the PWD element.	2019-06-19	not yet calculated	CVE-2019-11232 MISC
forgerock -- openam_and_am	OAuth 2.0 Authorization Server of ForgeRock Access Management (OpenAM) 13.5.0-13.5.1 and Access Management (AM) 5.0.0-5.1.1 does not correctly validate redirect_uri for some invalid requests, which allows attackers to perform phishing via an unvalidated redirect.	2019-06-19	not yet calculated	CVE-2017-14394 MISC
forgerock -- openam_and_am	Auth 2.0 Authorization Server of ForgeRock Access Management (OpenAM) 13.5.0-13.5.1 and Access Management (AM) 5.0.0-5.1.1 does not correctly validate redirect_uri for some invalid requests, which allows attackers to execute a script in the user's browser via reflected XSS.	2019-06-19	not yet calculated	CVE-2017-14395 MISC
freepbx -- freepbx	FreePBX 13 and 14 has SQL Injection in the DISA module via the hangup variable on the /admin/config.php?display=disa&view=form page.	2019-06-20	not yet calculated	CVE-2018-158

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				92 CONFIRM MISC
freepbx -- freepbx	An issue was discovered in FreePBX core before 3.0.122.43, 14.0.18.34, and 5.0.1beta4. By crafting a request for adding Asterisk modules, an attacker is able to store JavaScript commands in a module name.	2019-06-20	not yet calculated	CVE-2018-15891 CONFIRM MISC
glot.io -- glot-www	The default configuration of glot-www through 2018-05-19 allows remote attackers to execute arbitrary code because glot-code-runner supports os.system within a "python" "files" "content" JSON file.	2019-06-21	not yet calculated	CVE-2018-15747 MISC
helpy -- helpy	Helpy v2.1.0 has Stored XSS via the Ticket title.	2019-06-18	not yet calculated	CVE-2018-18886 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CCONFIRM
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an embedded web server potentially vulnerable to stored XSS in wireless configuration page	2019-06-17	not yet calculated	CVE-2019-6324 MISC
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an embedded web server potentially vulnerable to reflected XSS in wireless configuration page.	2019-06-17	not yet calculated	CVE-2019-6323 MISC
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an embedded web server that is potentially vulnerable to Cross-site Request Forgery.	2019-06-17	not yet calculated	CVE-2019-6325 MISC
hp -- color_laserjet_pro_m280	HP Color LaserJet Pro M280-M281 Multifunction Printer series	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
- m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	(before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an IPP Parser potentially vulnerable to Buffer Overflow.	06-17	calculated	2019-6327 MISC
hp -- color_laserjet_pro_m280 - m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have embedded web server attributes which may be potentially vulnerable to Buffer Overflow.	2019-06-17	not yet calculated	CVE-2019-6326 MISC
ibm -- sprectrum_protect_plus	IBM Spectrum Protect Plus 10.1.2 may display the vSnap CIFS password in the IBM Spectrum Protect Plus Joblog. This can result in an attacker gaining access to sensitive information as well as vSnap. IBM X-Force ID: 162173.	2019-06-19	not yet calculated	CVE-2019-4385 CONFIRM XF
libgcrypt -- libgcrypt	In Libgcrypt 1.8.4, the C implementation of AES is vulnerable to a flush-and-reload side-channel attack because physical addresses are available to other processes. (The C implementation is used on platforms where an assembly-	2019-06-19	not yet calculated	CVE-2019-12904 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	language implementation is unavailable.)			MISC MISC
london_trust_media -- private_internet_access_vpn_client_for_windows	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client 1.0.2 (build 02363) for Windows could allow an authenticated, local attacker to run arbitrary code with elevated privileges. On startup, the PIA Windows service (pia-service.exe) loads the OpenSSL library from %PROGRAMFILES%\Private Internet Access\libeay32.dll. This library attempts to load the C:\etc\ssl\openssl.cnf configuration file which does not exist. By default on Windows systems, authenticated users can create directories under C:\. A low privileged user can create a C:\etc\ssl\openssl.cnf configuration file to load a malicious OpenSSL engine library resulting in arbitrary code execution as SYSTEM when the service starts.	2019-06-21	not yet calculated	CVE-2019-12572 MISC MISC
netflix -- dial	Denial of Service (DOS) in Dial Reference Source Code Used before June 18th, 2019.	2019-06-21	not yet calculated	CVE-2019-100

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				28 CONFIRM
openstack -- magnum	OpenStack Magnum passes OpenStack credentials into the Heat templates creating its instances. While these should just be used for retrieving the instances' SSL certificates, they allow full API access, though and can be used to perform any API operation the user is authorized to perform.	2019-06-21	not yet calculated	CVE-2016-7404 MISC MISC CONFIRM MISC
opnsense -- opnsense	OPNsense 18.7.x before 18.7.7 has Incorrect Access Control.	2019-06-17	not yet calculated	CVE-2018-18958 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phoenix_contact -- axc_f_2152_and_axc_f_2152_starterkit_devices	An issue was discovered on Phoenix Contact AXC F 2152 (No.2404267) before 2019.0 LTS and AXC F 2152 STARTERKIT (No.1046568) before 2019.0 LTS devices. Unlimited physical access to the PLC may lead to a manipulation of SD cards data. SD card manipulation may lead to an authentication bypass opportunity.	2019-06-18	not yet calculated	CVE-2019-10998 CONFIRM
phoenix_contact -- axc_f_2152_and_axc_f_2152_starterkit_devices	An issue was discovered on Phoenix Contact AXC F 2152 (No.2404267) before 2019.0 LTS and AXC F 2152 STARTERKIT (No.1046568) before 2019.0 LTS devices. Protocol Fuzzing on PC WORX Engineer by a man in the middle attacker stops the PLC service. The device must be rebooted, or the PLC service must be restarted manually via a Linux shell.	2019-06-17	not yet calculated	CVE-2019-10997 CONFIRM
pix-link -- repeater/router_lv-wr09	An XSS issue on the PIX-Link Repeater/Router LV-WR09 with firmware v28K.MiniRouter.20180616 allows attackers to steal credentials without being connected to the network. The attack vector is a crafted ESSID.	2019-06-22	not yet calculated	CVE-2019-12933 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pydio -- pydio	Pydio Cells before 1.5.0 fails to neutralize '../' elements, allowing an attacker with minimum privilege to Upload files to, and Delete files/folders from, an unprivileged directory, leading to Privilege escalation.	2019-06-19	not yet calculated	CVE-2019-12901 MISC MISC
pydio -- pydio	Pydio Cells before 1.5.0, when supplied with a Name field in an unexpected Unicode format, fails to handle this and includes the database column/table name as pert of the error message, exposing sensitive information.	2019-06-19	not yet calculated	CVE-2019-12903 MISC MISC
pydio -- pydio	Pydio Cells before 1.5.0 does incomplete cleanup of a user's data upon deletion. This allows a new user, holding the same User ID as a deleted user, to restore the deleted user's data.	2019-06-19	not yet calculated	CVE-2019-12902 MISC MISC
rdk_management -- rdkb-20181217-1	A heap-based buffer overflow in cosa_dhcpv4_dml.c in the RDK	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	RDKB-20181217-1 CcspPandM module may allow attackers with login credentials to achieve remote code execution by crafting a long buffer in the "Comment" field of an IP reservation form in the admin panel. This is related to the CcspCommonLibrary module.	06-20	calculated	2019-6963 MISC
rdk_management -- rdkb-20181217-1	A shell injection issue in cosa_wifi_apis.c in the RDK RDKB-20181217-1 CcspWifiAgent module allows attackers with login credentials to execute arbitrary shell commands under the CcspWifiSsp process (running as root) if the platform was compiled with the ENABLE_FEATURE_MESHWIFI macro. The attack is conducted by changing the Wi-Fi network password to include crafted escape characters. This is related to the WebUI module.	2019-06-20	not yet calculated	CVE-2019-6962 MISC
rdk_management -- rdkb-20181217-1	Incorrect access control in actionHandlerUtility.php in the RDK RDKB-20181217-1 WebUI module allows a logged in user to control DDNS, QoS, RIP, and other privileged configurations (intended only for the network operator) by sending an HTTP POST to the PHP backend, because the page filtering for non-superuser (in header.php) is done	2019-06-20	not yet calculated	CVE-2019-6961 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	only for GET requests and not for direct AJAX calls.			
rdk_management -- rdkb-20181217-1	A heap-based buffer over-read in Service_SetParamStringValue in cosa_x_cisco_com_ddns_dml.c of the RDK RDKB-20181217-1 CcspPandM module may allow attackers with login credentials to achieve information disclosure and code execution by crafting an AJAX call responsible for DDNS configuration with an exactly 64-byte username, password, or domain, for which the buffer size is insufficient for the final '\0' character. This is related to the CcspCommonLibrary and WebUI modules.	2019-06-20	not yet calculated	CVE-2019-6964 MISC
redwoodhq -- redwoodhq	RedwoodHQ 2.5.5 does not require any authentication for database operations, which allows remote attackers to create admin users via a con.automationframework users insert_one call.	2019-06-19	not yet calculated	CVE-2019-12890 MISC MISC
shenzhen_cylan_technology -- clever_dog_smart_camer	On Shenzhen Cylan Clever Dog Smart Camera DOG-2W and DOG-2W-V4 devices, an attacker on the local network has	2019-06-20	not yet calc	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
a_dog-2w_and_dog-2w-v4	unauthenticated access to the internal SD card via the HTTP service on port 8000. The HTTP web server on the camera allows anyone to view or download the video archive recorded and saved on the external memory card attached to the device.		ulated	12919 MISC
shenzhen_cylan_technology -- clever_dog_smart_camera_dog-2w_and_dog-2w-v4	On Shenzhen Cylan Clever Dog Smart Camera DOG-2W and DOG-2W-V4 devices, an attacker on the network can login remotely to the camera and gain root access. The device ships with a hardcoded 12345678 password for the root account, accessible from a TELNET login prompt.	2019-06-20	not yet calculated	CVE-2019-12920 MISC
solarwinds -- serv-u_ftp_server	A privilege escalation vulnerability exists in SolarWinds Serv-U before 15.1.7 for Linux.	2019-06-17	not yet calculated	CVE-2019-12181 MISC MISC CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sony -- bravia_smart_tv_devices	The Photo Sharing Plus component on Sony Bravia TV through 8.587 devices has a Buffer Overflow.	2019-06-19	not yet calculated	CVE-2018-16595 MISC MISC
sony -- bravia_smart_tv_devices	The Photo Sharing Plus component on Sony Bravia TV through 8.587 devices allows Directory Traversal.	2019-06-19	not yet calculated	CVE-2018-16594 MISC MISC
sony -- bravia_smart_tv_devices	The Photo Sharing Plus component on Sony Bravia TV through 8.587 devices allows Shell Metacharacter Injection.	2019-06-19	not yet calculated	CVE-2018-16593 MISC MISC
sophos -- xg_firewall	A shell escape vulnerability in /webconsole/APIController in the	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	API Configuration component of Sophos XG firewall 17.0.8 MR-8 allows remote attackers to execute arbitrary OS commands via shell metachracters in the "X-Forwarded-for" HTTP header.	06-20	calculated	2018-16118 CONFIRM MISC MISC
sophos -- xg_firewall	SQL injection vulnerability in AccountStatus.jsp in Admin Portal of Sophos XG firewall 17.0.8 MR-8 allow remote authenticated attackers to execute arbitrary SQL commands via the "username" GET parameter.	2019-06-20	not yet calculated	CVE-2018-16116 CONFIRM MISC MISC
tp_link -- wr1043nd_devices	Stack-based buffer overflow in the httpd server of TP-Link WR1043nd (Firmware Version 3) allows remote attackers to execute arbitrary code via a malicious MediaServer request to /userRpm/MediaServerFoldersCfgRpm.htm.	2019-06-20	not yet calculated	CVE-2018-16119 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tufin -- securetrack	An issue was discovered in Tufin SecureTrack 18.1 with TufinOS 2.16 build 1179(Final). The Audit Report module is affected by a blind XXE vulnerability when a new Best Practices Report is saved using a special payload inside the xml input field. The XXE vulnerability is blind since the response doesn't directly display a requested file, but rather returns it inside the name data field when the report is saved. An attacker is able to view restricted operating system files. This issue affects all types of users: administrators or normal users.	2019-06-19	not yet calculated	CVE-2018-18406 MISC MISC MISC
tyto_software -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7.x.x and 8.0.0. A directory traversal (arbitrary file access) vulnerability exists in the web reports module. This allows an outside attacker to view contents of sensitive files.	2019-06-17	not yet calculated	CVE-2018-20470 MISC MISC
vtech -- storio_max_devices	VTech Storio Max before 56.D3JM6 allows remote command execution via shell metacharacters in an Android activity name. It exposes the storeintenttranslate.x service on port 1668 listening for requests on	2019-06-19	not yet calculated	CVE-2018-16618 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	localhost. Requests submitted to this service are checked for a string of random characters followed by the name of an Android activity to start. Activities are started by inserting their name into a string that is executed in a shell command. By inserting metacharacters this can be exploited to run arbitrary commands as root. The requests also match those of the HTTP protocol and can be triggered on any web page rendered on the device by requesting resources stored at an http://127.0.0.1:1668/ URI, as demonstrated by the http://127.0.0.1:1668/dacdb70556479813fab2d92896596eef?';{ping,example.org}' URL.			CMISC
wago -- multiple_devices	WAGO 852-303 before FW06, 852-1305 before FW06, and 852-1505 before FW03 devices contain hardcoded users and passwords that can be used to login via SSH and TELNET.	2019-06-17	not yet calculated	CVE-2019-12550 MISC MISC MISC
wago -- multiple_devices	WAGO 852-303 before FW06, 852-1305 before FW06, and 852-	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1505 before FW03 devices contain hardcoded private keys for the SSH daemon. The fingerprint of the SSH host key from the corresponding SSH daemon matches the embedded private key.	06-17	calculated	2019-12549 MISC MISC MISC
whatsapp -- whatsapp	When receiving calls using WhatsApp for Android, a missing size check when parsing a sender-provided packet allowed for a stack-based overflow. This issue affects WhatsApp for Android prior to 2.18.248 and WhatsApp Business for Android prior to 2.18.132.	2019-06-14	not yet calculated	CVE-2018-6349 BID MISC
wordpress -- wordpress	An issue was discovered in the update function in the wpForo Forum plugin before 1.5.2 for WordPress. A registered forum is able to escalate privilege to the forum administrator without any form of user interaction.	2019-06-19	not yet calculated	CVE-2018-16613 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	An arbitrary password reset issue was discovered in the Ultimate Member plugin 2.39 for WordPress. It is possible (due to lack of verification and correlation between the reset password key sent by mail and the user_id parameter) to reset the password of another user. One only needs to know the user_id, which is publicly available. One just has to intercept the password modification request and modify user_id. It is possible to modify the passwords for any users or admin WordPress Ultimate Members. This could lead to account compromise and privilege escalation.	2019-06-21	not yet calculated	CVE-2019-10270 MISC