Vulnerability Summary for the Week of February 15, 2021

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
accellion -- fta	Accellion FTA 9_12_411 and earlier is affected by OS command execution via a local web service call. The fixed version is FTA_9_12_416 and later.	2021-02-16	7.2	CVE-2021-27102 MISC MISC
accellion -- fta	Accellion FTA 9_12_370 and earlier is affected by OS command execution via a crafted POST request to various admin endpoints. The fixed version is FTA_9_12_380 and later.	2021-02-16	10	CVE-2021-27104 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accellion -- fta	Accellion FTA 9_12_411 and earlier is affected by SSRF via a crafted POST request to wmProgressstat.html. The fixed version is FTA_9_12_416 and later.	2021-02-16	7.5	CVE-2021-27103 MISC MISC
accellion -- fta	Accellion FTA 9_12_370 and earlier is affected by SQL injection via a crafted Host header in a request to document_root.html. The fixed version is FTA_9_12_380 and later.	2021-02-16	7.5	CVE-2021-27101 MISC MISC
advantech -- webaccess\/scada	An exploitable local privilege elevation vulnerability exists in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. In COM Server Application Privilege Escalation, an attacker can either replace binary or loaded modules to execute code with NT SYSTEM privilege.	2021-02-17	7.2	CVE-2020-13555 MISC
advantech -- webaccess\/scada	An exploitable local privilege elevation vulnerability exists in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. In webvrpcs Run Key Privilege Escalation in installation folder of WebAccess, an attacker can either replace binary or loaded	2021-02-17	7.2	CVE-2020-13553 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	modules to execute code with NT SYSTEM privilege.			
advantech -- webaccess\/scada	An exploitable local privilege elevation vulnerability exists in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. In privilege escalation via multiple service executables in installation folder of WebAccess, an attacker can either replace binary or loaded modules to execute code with NT SYSTEM privilege.	2021-02-17	7.2	CVE-2020-13552 MISC
advantech -- webaccess\/scada	An exploitable local privilege elevation vulnerability exists in the file system permissions of Advantech WebAccess/SCADA 9.0.1 installation. In privilege escalation via PostgreSQL executable, an attacker can either replace binary or loaded modules to execute code with NT SYSTEM privilege.	2021-02-17	7.2	CVE-2020-13551 MISC
citsmart -- citsmart	CITSmart before 9.1.2.23 allows LDAP Injection.	2021-02-15	7.5	CVE-2020-35775 MISC CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dlink -- dap-1860_firmware	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1860 firmware version 1.04B03 WiFi extenders. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HNAP service, which listens on TCP port 80 by default. When parsing the Authorization request header, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10880.	2021-02-12	8.3	CVE-2020-27864 MISC MISC
dlink -- dap-1860_firmware	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1860 firmware version 1.04B03 WiFi extenders. Authentication is not required to exploit this vulnerability. The specific flaw exists within the uhttpd service, which listens on TCP port 80 by default. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to	2021-02-12	8.3	CVE-2020-27865 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	escalate privileges and execute code in the context of the device. Was ZDI-CAN-10894.			
elecom -- wrc-300febk-s_firmware	ELECOM WRC-300FEBK-S allows an attacker with administrator rights to execute arbitrary OS commands via unspecified vectors.	2021-02-12	7.7	CVE-2021-20648 MISC MISC
iptime -- c200_firmware	The EFM ipTIME C200 IP Camera is affected by a Command Injection vulnerability in /login.cgi?logout=1 script. To exploit this vulnerability, an attacker can send a GET request that executes arbitrary OS commands via cookie value.	2021-02-17	7.7	CVE-2020-7848 MISC
limesurvey -- limesurvey	LimeSurvey before 4.0.0-RC4 allows SQL injection via the participant model.	2021-02-14	7.5	CVE-2019-25019 MISC MISC
logitec -- lan-w300n\/pgrb_firmware	Buffer overflow vulnerability in LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute an arbitrary OS command via unspecified vectors.	2021-02-12	7.7	CVE-2021-20640 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
logitec -- lan-w300n\/pgrb_firmware	LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors.	2021-02-12	7.7	CVE-2021-20639 MISC MISC
logitec -- lan-w300n\/pgrb_firmware	LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors.	2021-02-12	7.7	CVE-2021-20638 MISC MISC
microfocus -- operations_bridge_manager	Arbitrary code execution vulnerability on Micro Focus Operations Bridge Manager product, affecting versions 10.1x, 10.6x, 2018.05, 2018.11, 2019.05, 2019.11, 2020.05, 2020.10. The vulnerability could allow remote attackers to execute arbitrary code on an OBM server.	2021-02-12	10	CVE-2021-22504 MISC
nagios -- nagios_xi	Nagios XI version xi-5.7.5 is affected by OS command injection. The vulnerability exists in the file /usr/local/nagiosxi/html/includes/configwizards/cloud-vm/cloud-vm.inc.php due to improper sanitization of authenticated user-controlled input by a single HTTP request, which can lead to OS	2021-02-15	9	CVE-2021-25298 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	command injection on the Nagios XI server.			
nagios -- nagios_xi	Nagios XI version xi-5.7.5 is affected by OS command injection. The vulnerability exists in the file /usr/local/nagiosxi/html/includes/configwizards/switch/switch.inc.php due to improper sanitization of authenticated user-controlled input by a single HTTP request, which can lead to OS command injection on the Nagios XI server.	2021-02-15	9	CVE-2021-25297 MISC MISC MISC
nagios -- nagios_xi	Nagios XI version xi-5.7.5 is affected by OS command injection. The vulnerability exists in the file /usr/local/nagiosxi/html/includes/configwizards/windowswmi/windowswmi.inc.php due to improper sanitization of authenticated user-controlled input by a single HTTP request, which can lead to OS command injection on the Nagios XI server.	2021-02-15	9	CVE-2021-25296 MISC MISC MISC
netgear -- ac2100_firmware	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6020, R6080, R6120, R6220, R6260,	2021-02-12	7.7	CVE-2020-27867 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	R6700v2, R6800, R6900v2, R7450, JNR3210, WNR2020, Nighthawk AC2100, and Nighthawk AC2400 firmware version 1.2.0.62_1.0.1 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the mini_httpd service, which listens on TCP port 80 by default. When parsing the funjsq_access_token parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-11653.			
netgear -- ac2100_firmware	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6020, R6080, R6120, R6220, R6260, R6700v2, R6800, R6900v2, R7450, JNR3210, WNR2020, Nighthawk AC2100, and Nighthawk AC2400 firmware version 1.2.0.62_1.0.1 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within	2021-02-12	8.3	CVE-2020-27866 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the mini_httpd service, which listens on TCP port 80 by default. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-11355.			
netgear -- cbk40_firmware	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR Orbi 2.5.1.16 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UA_Parser utility. A crafted Host Name option in a DHCP request can trigger execution of a system call composed from a user-supplied string. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-11076.	2021-02-12	8.3	CVE-2020-27861 MISC MISC
pelco -- digital_sentry_server	DSUtility.dll in Pelco Digital Sentry Server before 7.19.67 has an arbitrary file write vulnerability. The AppendToTextFile method doesn't check if it's being called from the application or from a malicious user. The vulnerability is triggered when	2021-02-12	8.8	CVE-2021-27197 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a remote attacker crafts an HTML page (e.g., with "OBJECT classid=" and "<SCRIPT language='vbscript'>") to overwrite arbitrary files.			
pystemon_project -- pystemon	config.py in pystemon before 2021-02-13 allows code execution via YAML deserialization because SafeLoader and safe_load are not used.	2021-02-14	7.5	CVE-2021-27213 MISC MISC
qognify -- ocularis	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Qognify Ocularis 5.9.0.395. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of serialized objects provided to the EventCoordinator endpoint. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-11257.	2021-02-12	10	CVE-2020-27868 MISC MISC
racom -- m\!dge_cellular	Racom's MIDGE Firmware 4.4.40.105 contains an issue	2021-02-16	7.2	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_router_firmware	that allows for privilege escalation via configd.			20075 MISC
sdg -- pnpscada	PNPSCADA 2.200816204020 allows SQL injection via parameter 'interf' in /browse.jsp. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.	2021-02-16	7.5	CVE-2020-24841 MISC MISC
solarwinds -- network_performance_monitor	This vulnerability allows remote attackers to escalate privileges on affected installations of SolarWinds Network Performance Monitor 2020 HF1, NPM: 2020.2. Authentication is required to exploit this vulnerability. The specific flaw exists within the WriteToFile method. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges and reset the password for the Admin user. Was ZDI-CAN-11804.	2021-02-12	9	CVE-2020-27869 MISC
zscaler -- client_connector	The Zscaler Client Connector prior to 3.1.0 did not sufficiently validate RPC clients, which allows a local	2021-02-16	7.2	CVE-2020-11635 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	adversary to execute code with system privileges or perform limited actions for which they did not have privileges.			

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
advantech -- webaccess\/scada	A local file inclusion vulnerability exists in the installation functionality of Advantech WebAccess/SCADA 9.0.1. A specially crafted application can lead to information disclosure. An attacker can send an authenticated HTTP request to trigger this vulnerability.	2021-02-17	4	CVE-2020-13550 MISC
apache -- thrift	In Apache Thrift 0.9.3 to 0.13.0, malicious RPC clients could send short messages which would result in a large memory allocation, potentially leading to denial of service.	2021-02-12	5	CVE-2020-13949 MLIST MLIST MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MLIST MLIST MISC MLIST MLIST MLIST MLIST MLIST
atlassian -- data_center	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to view custom field options via an Information Disclosure vulnerability in the /rest/api/2/customFieldOption/ endpoint. The affected versions are before version 8.15.0.	2021-02-15	5	CVE-2020-36237 MISC
atlassian -- data_center	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to enumerate Jira projects via an Information Disclosure vulnerability in the Jira Projects plugin report page. The affected versions are before version 8.5.11, from version 8.6.0 before 8.13.3, and from version 8.14.0 before 8.14.1.	2021-02-15	4	CVE-2020-29451 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- jira	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to view custom field and custom SLA names via an Information Disclosure vulnerability in the mobile site view. The affected versions are before version 8.13.2, and from version 8.14.0 before 8.14.1.	2021-02-15	5	CVE-2020-36235 MISC
atlassian -- jira	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the ViewWorkflowSchemes.jspa and ListWorkflows.jspa endpoints. The affected versions are before version 8.5.11, from version 8.6.0 before 8.13.3, and from version 8.14.0 before 8.15.0.	2021-02-15	4.3	CVE-2020-36236 MISC
changjia_property_management_system_project -- changjia_property_management_system	The CGE property management system contains SQL Injection vulnerabilities. Remote attackers can inject SQL commands into the parameters in Cookie and obtain data in the database without privilege.	2021-02-17	5	CVE-2021-22856 CONFIRM MISC
changjia_property_management_system_project	The CGE page with download function contains a Directory Traversal vulnerability.	2021-02-17	5	CVE-2021-22857

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
-- changjia_property_management_system	Attackers can use this loophole to download system files arbitrarily.			CONFIRM MISC
deepnetsecurity -- dualshield	DualShield 5.9.8.0821 allows username enumeration on its login form. A valid username results in prompting for the password, whereas an invalid one will produce an "unknown username" error message.	2021-02-16	5	CVE-2020-28918 MISC MISC
dlink -- dva-2800_firmware	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DVA-2800 and DSL-2888A firmware version 2.3 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the dhttpd service, which listens on TCP port 8008 by default. When parsing the path parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-10911.	2021-02-12	5.8	CVE-2020-27862 MISC MISC
elecom -- file_manager	Directory traversal vulnerability in ELECOM File Manager all versions allows	2021-02-12	6.4	CVE-2021-20651

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote attackers to create an arbitrary file or overwrite an existing file in a directory which can be accessed with the application privileges via unspecified vectors.			MISC MISC
elecom -- ld-ps\/u1_firmware	Improper access control vulnerability in ELECOM LD-PS/U1 allows remote attackers to change the administrative password of the affected device by processing a specially crafted request.	2021-02-12	5	CVE-2021-20643 MISC MISC
elecom -- ncc-ewf100rmwh2_firmware	Cross-site request forgery (CSRF) vulnerability in ELECOM NCC-EWF100RMWH2 allows remote attackers to hijack the authentication of administrators and execute an arbitrary request via unspecified vector. As a result, the device settings may be altered and/or telnet daemon may be started.	2021-02-12	4.3	CVE-2021-20650 MISC MISC
elecom -- wrc-1467ghbk-a_firmware	ELECOM WRC-1467GHBK-A allows arbitrary scripts to be executed on the user's web browser by displaying a specially crafted SSID on the web setup page.	2021-02-12	4.3	CVE-2021-20644 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elecom -- wrc-300febk-a_firmware	Cross-site scripting vulnerability in ELECOM WRC-300FEBK-A allows remote authenticated attackers to inject arbitrary script via unspecified vectors.	2021-02-12	4.3	CVE-2021-20645 MISC MISC
elecom -- wrc-300febk-a_firmware	Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-A allows remote attackers to hijack the authentication of administrators and execute an arbitrary request via unspecified vector. As a result, the device settings may be altered and/or telnet daemon may be started.	2021-02-12	4.3	CVE-2021-20646 MISC MISC
elecom -- wrc-300febk-s_firmware	ELECOM WRC-300FEBK-S contains an improper certificate validation vulnerability. Via a man-in-the-middle attack, an attacker may alter the communication response. As a result, an arbitrary OS command may be executed on the affected device.	2021-02-12	5.8	CVE-2021-20649 MISC MISC
elecom -- wrc-300febk-s_firmware	Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-S allows remote attackers to hijack the authentication of administrators and execute an arbitrary request via unspecified vector. As a result,	2021-02-12	4.3	CVE-2021-20647 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the device settings may be altered and/or telnet daemon may be started.			
f5 -- access_policy_manager_clients	In Edge Client version 7.2.x before 7.2.1.1, 7.1.9.x before 7.1.9.8, and 7.1.x-7.1.8.x before 7.1.8.5, an untrusted search path vulnerability in the BIG-IP APM Client Troubleshooting Utility (CTU) for Windows could allow an attacker to load a malicious DLL library from its current directory. User interaction is required to exploit this vulnerability in that the victim must run this utility on the Windows system. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	2021-02-12	6.9	CVE-2021-22980 MISC
f5 -- big-ip_access_policy_manager	On BIG-IP version 16.0.x before 16.0.1, 15.1.x before 15.1.1, 14.1.x before 14.1.2.8, 13.1.x before 13.1.3.5, and all 12.1.x versions, a reflected Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility when Fraud Protection Service is provisioned and allows an attacker to execute JavaScript in the context of the current logged-in user. Note: Software	2021-02-12	4.3	CVE-2021-22979 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions which have reached End of Software Development (EoSD) are not evaluated.			
f5 -- big-ip_access_policy_manager	On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2.1, and 14.1.x before 14.1.3.1, under some circumstances, Traffic Management Microkernel (TMM) may restart on the BIG-IP system while passing large bursts of traffic. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	2021-02-12	4.3	CVE-2021-22975 MISC
f5 -- big-ip_access_policy_manager	On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, and 13.1.x before 13.1.3.6 and all versions of BIG-IQ 7.x and 6.x, an authenticated attacker with access to iControl REST over the control plane may be able to take advantage of a race condition to execute commands with an elevated privilege level. This vulnerability is due to an incomplete fix for CVE-2017-6167. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	2021-02-12	6	CVE-2021-22974 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
f5 -- big-ip_access_policy_manager	On all versions of BIG-IP 12.1.x and 11.6.x, the original TLS protocol includes a weakness in the master secret negotiation that is mitigated by the Extended Master Secret (EMS) extension defined in RFC 7627. TLS connections that do not use EMS are vulnerable to man-in-the-middle attacks during renegotiation. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	2021-02-12	5.8	CVE-2021-22981 MISC
f5 -- big-ip_access_policy_manager	On BIG-IP version 16.0.0-16.0.1 and 14.1.2.4-14.1.3, cooperation between malicious HTTP client code and a malicious server may cause TMM to restart and generate a core file. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	2021-02-12	5	CVE-2021-22977 MISC
f5 -- big-ip_access_policy_manager	On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, 13.1.x before 13.1.3.5, and all 12.1.x versions, JSON parser function does not protect against out-of-bounds memory accesses or writes. Note: Software versions which have reached End of Software	2021-02-12	5	CVE-2021-22973 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Development (EoSD) are not evaluated.			
f5 -- big-ip_advanced_web_application_firewall	On BIG-IP Advanced WAF and ASM version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, 13.1.x before 13.1.3.6, and all 12.1.x versions, when the BIG-IP ASM system processes WebSocket requests with JSON payloads, an unusually large number of parameters can cause excessive CPU usage in the BIG-IP ASM bd process. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	2021-02-12	5	CVE-2021-22976 MISC
f5 -- big-ip_advanced_web_application_firewall	On BIG-IP Advanced WAF and ASM version 15.1.x before 15.1.0.2, 15.0.x before 15.0.1.4, 14.1.x before 14.1.2.5, 13.1.x before 13.1.3.4, 12.1.x before 12.1.5.2, and 11.6.x before 11.6.5.2, when receiving a unauthenticated client request with a maliciously crafted URI, a BIG-IP Advanced WAF or ASM virtual server configured with a DoS profile with Proactive Bot Defense (versions prior to 14.1.0), or a Bot Defense profile (versions 14.1.0 and later), may subject clients and web servers to Open	2021-02-12	5.8	CVE-2021-22984 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Redirection attacks. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.			
f5 -- big-ip_domain_name_system	On BIG-IP DNS and GTM version 13.1.x before 13.1.0.4, and all versions of 12.1.x and 11.6.x, big3d does not securely handle and parse certain payloads resulting in a buffer overflow. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	2021-02-12	6.5	CVE-2021-22982 MISC
foxitsoftware -- foxit_reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.0.1.35811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11727.	2021-02-12	6.8	CVE-2020-27860 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
horde -- groupware	An XSS issue was discovered in Horde Groupware Webmail Edition through 5.2.22 (where the Horde_Text_Filter library before 2.3.7 is used). The attacker can send a plain text e-mail message, with JavaScript encoded as a link or email that is mishandled by preProcess in Text2html.php, because bespoke use of \x00\x00\x00 and \x01\x01\x01 interferes with XSS defenses.	2021-02-14	4.3	CVE-2021-26929 MISC MLIST CONFIRM MISC MISC
ibm -- spectrum_protect_operations_center	IBM Spectrum Protect Operations Center 7.1 and 8.1could allow a remote attacker to execute arbitrary code on the system, caused by improper parameter validation. By creating an unspecified servlet request with specially crafted input parameters, an attacker could exploit this vulnerability to load a malicious .dll with elevated privileges. IBM X-Force ID: 192155.	2021-02-15	5.2	CVE-2020-4955 XF CONFIRM
ibm -- spectrum_protect_operations_center	IBM Spectrum Protect Operations Center 7.1 and 8.1 could allow a remote attacker to bypass authentication restrictions, caused by improper session validation . By using the configuration panel to obtain a valid session using an attacker controlled	2021-02-15	4.8	CVE-2020-4954 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	IBM Spectrum Protect server, an attacker could exploit this vulnerability to bypass authentication and gain access to a limited number of debug functions, such as logging levels. IBM X-Force ID: 192153.			
logitec -- lan-w300n\/pr5b_firmware	Cross-site request forgery (CSRF) vulnerability in LOGITEC LAN-W300N/PR5B allows remote attackers to hijack the authentication of administrators via a specially crafted URL. As a result, unintended operations to the device such as changes of the device settings may be conducted.	2021-02-12	4.3	CVE-2021-20636 MISC MISC
logitec -- lan-w300n\/pr5b_firmware	Improper check or handling of exceptional conditions in LOGITEC LAN-W300N/PR5B allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted URL.	2021-02-12	4.3	CVE-2021-20637 MISC MISC
logitec -- lan-w300n\/rs_firmware	Cross-site request forgery (CSRF) vulnerability in LOGITEC LAN-W300N/RS allows remote attackers to hijack the authentication of administrators via a specially crafted URL. As a result, unintended operations to the	2021-02-12	4.3	CVE-2021-20641 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device such as changes of the device settings may be conducted.			
logitec -- lan-w300n\/rs_firmware	Improper check or handling of exceptional conditions in LOGITEC LAN-W300N/RS allows a remote attacker to cause a denial-of-service (DoS) condition by sending a specially crafted URL.	2021-02-12	4.3	CVE-2021-20642 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. An incomplete filter applied to a database response allows an authenticated attacker to gain non-public information about other users and devices in the account.	2021-02-16	4	CVE-2020-35568 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is an unauthenticated open redirect in the redirect.php.	2021-02-16	5.8	CVE-2020-35560 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. The login pages	2021-02-16	5	CVE-2020-35565 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bruteforce detection is disabled by default.			
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is an outdated and unused component allowing for malicious user input of active code.	2021-02-16	5	CVE-2020-35564 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is an unused function that allows an authenticated attacker to use up all available IPs of an account and thus not allow creation of new devices and users.	2021-02-16	4	CVE-2020-35559 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is an SSRF in thein the MySQL access check, allowing an attacker to scan for open ports and gain some information about possible credentials.	2021-02-16	5	CVE-2020-35558 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE	2021-02-16	5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mymbCONNECT24 and mbCONNECT24 through 2.6.2. An unauthenticated attacker is able to access files (that should have been restricted) via forceful browsing.			35570 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is a self XSS issue with a crafted cookie in the login page.	2021-02-16	4.3	CVE-2020-35569 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is an SSRF in the HA module allowing an unauthenticated attacker to scan for open ports.	2021-02-16	5	CVE-2020-35561 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. The software uses a secure password for database access, but this password is shared across instances.	2021-02-16	4.6	CVE-2020-35567 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE	2021-02-16	4	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mymbCONNECT24 and mbCONNECT24 software in all versions through 2.6.2. Inproper use of access validation allows a logged in user to see devices in the account he should not have access to.			35557 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. An attacker can read arbitrary JSON files via Local File Inclusion.	2021-02-16	5	CVE-2020-35566 MISC MISC
nagios -- nagios_xi	Nagios XI version xi-5.7.5 is affected by cross-site scripting (XSS). The vulnerability exists in the file /usr/local/nagiosxi/html/admin/sshterm.php due to improper sanitization of user-controlled input. A maliciously crafted URL, when clicked by an admin user, can be used to steal his/her session cookies or it can be chained with the previous bugs to get one-click remote command execution (RCE) on the Nagios XI server.	2021-02-15	4.3	CVE-2021-25299 MISC MISC MISC
online_book_store_project -- online_book_store	The id parameter in detail.php of Online Book Store v1.0 is vulnerable to union-based blind SQL injection, which leads to	2021-02-17	5	CVE-2020-36003 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the ability to retrieve all databases.			MISC MISC
open-emr -- openemr	A SQL injection vulnerability in interface/usergroup/usergroup_admin.php in OpenEMR before 5.0.2.5 allows a remote authenticated attacker to execute arbitrary SQL commands via the schedule_facility parameter when restrict_user_facility=on is in global settings.	2021-02-15	6.5	CVE-2020-29142 MISC MISC MISC MISC MISC
openzfs -- openzfs	An issue was discovered in OpenZFS through 2.0.3. When an NFS share is exported to IPv6 addresses via the sharenfs feature, there is a silent failure to parse the IPv6 address data, and access is allowed to everyone. IPv6 restrictions from the configuration are not applied.	2021-02-12	5	CVE-2013-20001 MISC MISC
php -- php	In PHP versions 7.3.x below 7.3.27, 7.4.x below 7.4.15 and 8.0.x below 8.0.2, when using SOAP extension to connect to a SOAP server, a malicious SOAP server could return malformed XML data as a response that would cause PHP to access a null pointer and thus cause a crash.	2021-02-15	5	CVE-2021-21702 CONFIRM DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
php -- php	In PHP versions 7.3.x below 7.3.26, 7.4.x below 7.4.14 and 8.0.0, when validating URL with functions like filter_var($url, FILTER_VALIDATE_URL), PHP will accept an URL with invalid password as valid URL. This may lead to functions that rely on URL being valid to mis-parse the URL and produce wrong data as components of the URL.	2021-02-15	5	CVE-2020-7071 CONFIRM DEBIAN
seat-reservation-system_project -- seat-reservation-system	Seat-Reservation-System 1.0 has a SQL injection vulnerability in index.php in the id and file parameters where attackers can obtain sensitive database information.	2021-02-17	5	CVE-2020-36002 MISC MISC MISC
secomea -- sitemanager_embedded	A vulnerability in SiteManager-Embedded (SM-E) Web server which may allow attacker to construct a URL that if visited by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application. This issue affects all versions and variants of SM-E prior to version 9.3	2021-02-16	4.3	CVE-2020-29025 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tp-link -- archer_c5v_firmware	TP-Link Archer C5v 1.7_181221 devices allows remote attackers to retrieve cleartext credentials via [USER_CFG#0,0,0,0,0,0#0,0,0,0,0,0]0,0 to the /cgi?1&5 URI.	2021-02-13	4	CVE-2021-27210 MISC
xn--b1agzlht -- fx_aggregator_terminal_client	The Sovremennye Delovye Tekhnologii FX Aggregator terminal client 1 allows attackers to cause a denial of service (access suspended for five hours) by making five invalid login attempts to a victim's account.	2021-02-12	5	CVE-2021-27188 MISC MISC
xn--b1agzlht -- fx_aggregator_terminal_client	The Sovremennye Delovye Tekhnologii FX Aggregator terminal client 1 stores authentication credentials in cleartext in login.sav when the Save Password box is checked.	2021-02-12	5	CVE-2021-27187 MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- data_center	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting	2021-02-15	3.5	CVE-2020-36234 N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(XSS) vulnerability in the Screens Modal view. The affected versions are before version 8.5.11, from version 8.6.0 before 8.13.3, and from version 8.14.0 before 8.15.0.			
blackcat-cms -- blackcat_cms	The admin panel in BlackCat CMS 1.3.6 allows stored XSS (by an admin) via the Display Name field to backend/preferences/ajax_save.php.	2021-02-16	3.5	CVE-2021-27237 MISC MISC MISC
dlink -- dva-2800_firmware	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link DVA-2800 and DSL-2888A firmware version 2.3 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the dhttpd service, which listens on TCP port 8008 by default. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-10912.	2021-02-12	3.3	CVE-2020-27863 MISC MISC
f5 -- big-ip_access_policy_manager	On BIG-IP version 16.0.x before 16.0.1, 15.1.x before 15.1.1, 14.1.x before 14.1.3.1,	2021-02-12	2.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	13.1.x before 13.1.3.5, and all 12.1.x and 11.6.x versions, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of BIG-IP if the victim user is granted the admin role. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.			22978 MISC
f5 -- big-ip_advanced_firewall_manager	On BIG-IP AFM version 15.1.x before 15.1.1, 14.1.x before 14.1.3.1, and 13.1.x before 13.1.3.5, authenticated users accessing the Configuration utility for AFM are vulnerable to a cross-site scripting attack if they attempt to access a maliciously-crafted URL. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	2021-02-12	3.5	CVE-2021-22983 MISC
ibm -- maximo_for_civil_infrastructure	IBM Maximo for Civil Infrastructure 7.6.2 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	2021-02-18	3.5	CVE-2021-20446 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	session. IBM X-Force ID: 196622.			
ibm -- spectrum_protect_operations_center	IBM Spectrum Protect Operations Center 7.1 and 8.1 is vulnerable to a denial of service, caused by a RPC that allows certain cache values to be set and dumped to a file. By setting a grossly large cache value and dumping that cached value to a file multiple times, a remote attacker could exploit this vulnerability to cause the consumption of all memory resources. IBM X-Force ID: 192156.	2021-02-15	2.3	CVE-2020-4956 XF CONFIRM
logitec -- lan-wh450n\/gr_firmware	Improper restriction of excessive authentication attempts in LOGITEC LAN-WH450N/GR allows an attacker in the wireless range of the device to recover PIN and access the network.	2021-02-12	3.3	CVE-2021-20635 MISC MISC
mbconnectline -- mbconnect24	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.2. There is an incomplete XSS filter allowing an attacker to inject crafted malicious code into the page.	2021-02-16	3.5	CVE-2020-35563 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nfstream -- nfstream	An issue was discovered in NFStream 5.2.0. Because some allocated modules are not correctly freed, if the nfstream object is directly destroyed without being used after it is created, it will cause a memory leak that may result in a local denial of service (DoS).	2021-02-16	2.1	CVE-2020-25340 MISC
peel -- peel_shopping	A Stored Cross Site Scripting(XSS) Vulnerability was discovered in PEEL SHOPPING 9.3.0 which is publicly available. The user supplied input containing polyglot payload is echoed back in javascript code in HTML response. This allows an attacker to input malicious JavaScript which can steal cookie, redirect them to other malicious website, etc.	2021-02-12	3.5	CVE-2021-27190 MISC MISC MISC
racom -- m\!dge_cellular_router_firmware	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scriptings attacks via the sms.php dialogs.	2021-02-16	3.5	CVE-2021-20071 MISC
racom -- m\!dge_cellular_router_firmware	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scriptings attacks via the virtualization.php dialogs.	2021-02-16	3.5	CVE-2021-20070 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
racom -- m\!dge_cellular_router_firmware	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scripting attacks via the regionalSettings.php dialogs.	2021-02-16	3.5	CVE-2021-20069 MISC
racom -- m\!dge_cellular_router_firmware	Racom's MIDGE Firmware 4.4.40.105 contains an issue that allows attackers to conduct cross-site scripting attacks via the error handling functionality of web pages.	2021-02-16	3.5	CVE-2021-20068 MISC
secomea -- sitemanager_1129_firmware	Cross-site Scripting (XSS) vulnerability in GUI of Secomea SiteManager could allow an attacker to cause an XSS Attack. This issue affects: Secomea SiteManager all versions prior to 9.3.	2021-02-16	3.5	CVE-2020-29027 MISC
tp-link -- archer_c5v_firmware	In the management interface on TP-Link Archer C5v 1.7_181221 devices, credentials are sent in a base64 format over cleartext HTTP.	2021-02-13	3.6	CVE-2021-27209 MISC