Vulnerability Summary for the Week of July 26, 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
adobe -- after_effects	Adobe After Effects version 18.1 (and earlier) is affected by an Uncontrolled Search Path element vulnerability. An unauthenticated attacker could exploit this to to plant custom binaries and execute them with System permissions. Exploitation of this issue requires user interaction.	2021-06-28	9.3	CVE-2021-28570 MISC
adobe -- after_effects	After Effects version 18.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in	2021-06-28	9.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			28586 MISC
adobe -- robohelp_server	Adobe RoboHelp Server version 2019.0.9 (and earlier) is affected by a Path Traversal vulnerability when parsing a crafted HTTP POST request. An authenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction.	2021-06-28	9	CVE-2021-28588 MISC
chamilo -- chamilo	main/inc/ajax/model.ajax.php in Chamilo through 1.11.14 allows SQL Injection via the searchField, filters, or filters2 parameter.	2021-06-28	7.5	CVE-2021-34187 MISC MISC MISC MISC
cnesty -- helpcom	A vulnerability of Helpcom could allow an unauthenticated attacker to execute arbitrary command. This vulnerability exists due to insufficient validation of	2021-06-29	7.5	CVE-2020-7871 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the parameter. This issue affects: Cnesty Helpcom 10.0 versions prior to.			
eclipse -- birt	In Eclipse BIRT versions 4.8.0 and earlier, an attacker can use query parameters to create a JSP file which is accessible from remote (current BIRT viewer dir) to inject JSP code into the running instance.	2021-06-25	7.5	CVE-2021-34427 CONFIRM
fatek -- winproladder	FATEK Automation WinProladder Versions 3.30 and prior do not properly restrict operations within the bounds of a memory buffer, which may allow an attacker to execute arbitrary code.	2021-06-29	7.5	CVE-2021-32992 MISC
fatek -- winproladder	FATEK Automation WinProladder Versions 3.30 and prior are vulnerable to an out-of-bounds write, which may allow an attacker to execute arbitrary code.	2021-06-29	7.5	CVE-2021-32988 MISC
fatek -- winproladder	FATEK Automation WinProladder Versions 3.30 and prior are vulnerable to an out-of-bounds read, which may allow an attacker to execute arbitrary code.	2021-06-29	7.5	CVE-2021-32990 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fidelissecurity -- deception	Vulnerability in the CommandPost, Collector, and Sensor components of Fidelis Network and Deception enables an attacker with user level access to the CLI to inject root level commands into the component and neighboring Fidelis components. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability.	2021-06-25	9	CVE-2021-35047 CONFIRM
fidelissecurity -- deception	Vulnerability in Fidelis Network and Deception CommandPost enables unauthenticated SQL injection through the web interface. The vulnerability could lead to exposure of authentication tokens in some versions of Fidelis software. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability.	2021-06-25	7.5	CVE-2021-35048 CONFIRM
helpu -- helpu	A remote code execution vulnerability exists in helpUS(remote administration tool) due to improper validation of parameter of ShellExecutionExA function used for login.	2021-06-29	10	CVE-2020-7868 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- anyoffice	There is a deserialization vulnerability in Huawei AnyOffice V200R006C10. An attacker can construct a specific request to exploit this vulnerability. Successfully exploiting this vulnerability, the attacker can execute remote malicious code injection and to control the device.	2021-06-29	9.3	CVE-2021-22439 MISC
inkdrop -- inkdrop	Inkdrop versions prior to v5.3.1 allows an attacker to execute arbitrary OS commands on the system where it runs by loading a file or code snippet containing an invalid iframe into Inkdrop.	2021-06-28	9.3	CVE-2021-20745 MISC MISC MISC
mastersoft -- zook	An improper input validation vulnerability of ZOOK software (remote administration tool) could allow a remote attacker to create arbitrary file. The ZOOK viewer has the "Tight file CMD" function to create file. An attacker could create and execute arbitrary file in the ZOOK agent program using "Tight file CMD" without authority.	2021-06-29	9	CVE-2020-7869 MISC
mcafee -- mvision_edr	A command injection vulnerability in MVISION EDR (MVEDR) prior to 3.4.0 allows an authenticated	2021-06-29	9	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	MVEDR administrator to trigger the EDR client to execute arbitrary commands through PowerShell using the EDR functionality 'execute reaction'.			31838 CONFIRM
miniaudio_project -- miniaudio	Miniaudio 0.10.35 has a Double free vulnerability that could cause a buffer overflow in ma_default_vfs_close__stdio in miniaudio.h.	2021-06-25	7.5	CVE-2021-34184 CONFIRM
misp -- misp	app/View/Elements/genericElements/IndexTable/Fields/generic_field.ctp in MISP 2.4.144 does not sanitize certain data related to generic-template:index.	2021-06-25	7.5	CVE-2021-35502 MISC
narou_project -- narou	Narou (aka Narou.rb) before 3.8.0 allows Ruby Code Injection via the title name or author name of a novel.	2021-06-28	7.5	CVE-2021-35514 MISC MISC
naviwebs -- navigate_cms	SQL Injection vulnerability in NavigateCMS 2.9 via the URL encoded GET input category in navigate.php.	2021-06-28	7.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				23711 MISC
online_pet_shop_web_application_project -- online_pet_shop_web_application	Online Pet Shop We App 1.0 is vulnerable to remote SQL injection and shell upload	2021-06-28	7.5	CVE-2021-35456 MISC MISC
pandorafms -- pandora_fms	PandoraFMS <=7.54 allows arbitrary file upload, it leading to remote command execution via the File Manager. To bypass the built-in protection, a relative path is used in the requests.	2021-06-25	7.5	CVE-2021-34074 MISC
phoenixcontact -- axl_f_bk_pn_tps_xc_firmware	In certain devices of the Phoenix Contact AXL F BK and IL BK product families an undocumented password protected FTP access to the root directory exists.	2021-06-25	7.5	CVE-2021-33540 CONFIRM
phoenixcontact -- fl_switch_smcs_16tx_firmware	In Phoenix Contact FL SWITCH SMCS series products in multiple versions if an attacker sends a hand-crafted TCP-Packet with the Urgent-Flag set and the Urgent-	2021-06-25	7.8	CVE-2021-21005

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Pointer set to 0, the network stack will crash. The device needs to be rebooted afterwards.			CONFIRM
phoenixcontact -- ilc1x0_firmware	Phoenix Contact Classic Line Controllers ILC1x0 and ILC1x1 in all versions/variants are affected by a Denial-of-Service vulnerability. The communication protocols and device access do not feature authentication measures. Remote attackers can use specially crafted IP packets to cause a denial of service on the PLC's network communication module. A successful attack stops all network communication. To restore the network connectivity the device needs to be restarted. The automation task is not affected.	2021-06-25	7.8	CVE-2021-33541 CONFIRM
securepoint -- openvpn-client	Securepoint SSL VPN Client v2 before 2.0.32 on Windows has unsafe configuration handling that enables local privilege escalation to NT AUTHORITY\SYSTEM. A non-privileged local user can modify the OpenVPN configuration stored under "%APPDATA%\Securepoint SSL VPN" and add a external script file that is executed as privileged user.	2021-06-28	7.2	CVE-2021-35523 MISC MISC FULLDISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenable -- nessus	Nessus versions 8.13.2 and earlier were found to contain a privilege escalation vulnerability which could allow a Nessus administrator user to upload a specially crafted file that could lead to gaining administrator privileges on the Nessus host.	2021-06-29	7.2	CVE-2021-20079 MISC
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable use of hard-coded credentials vulnerability exists in multiple iw_* utilities. The device operating system contains an undocumented encryption password, allowing for the creation of custom diagnostic scripts. An attacker can send diagnostic scripts while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33531 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable privilege escalation vulnerability exists in the iw_console functionality. A specially crafted menu selection string can cause an escape from the restricted console, resulting in system access as the root user. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33528 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in encrypted diagnostic script functionality of the devices. A specially crafted diagnostic script file can cause arbitrary busybox commands to be executed, resulting in remote control over the device. An attacker can send diagnostic while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33530 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in the hostname functionality. A specially crafted entry to network configuration information can cause execution of arbitrary system commands, resulting in full control of the device. An attacker can send various requests while authenticated as a high privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33534 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in the iw_webs functionality. A specially crafted diagnostic script file name can cause user input to be reflected in a subsequent iw_system call, resulting in remote control over the device. An attacker can send	2021-06-25	9	CVE-2021-33532 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	commands while authenticated as a low privilege user to trigger this vulnerability.			
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in the iw_webs functionality. A specially crafted iw_serverip parameter can cause user input to be reflected in a subsequent iw_system call, resulting in remote control over the device. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33533 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable improper access control vulnerability exists in the iw_webs account settings functionality. A specially crafted user name entry can cause the overwrite of an existing user account password, resulting in remote shell access to the device as that user. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	9	CVE-2021-33538 CONFIRM
wincred_project -- wincred	This affects all versions of package wincred. If attacker-controlled user input is given to the getCredential	2021-06-28	7.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.			23399 MISC MISC
zohocorp -- manageengine_adselfservice_plus	Zoho ManageEngine ADSelfService Plus through 6101 is vulnerable to unauthenticated Remote Code Execution while changing the password.	2021-06-25	7.5	CVE-2021-28958 MISC MISC
zohocorp -- manageengine_servicedesk_plus_msp	Zoho ManageEngine ServiceDesk Plus MSP before 10521 is vulnerable to Server-Side Request Forgery (SSRF).	2021-06-29	7.5	CVE-2021-31531 CONFIRM MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- after_effects	After Effects versions 18.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	4.3	CVE-2021-28587 MISC
adobe -- animate	Adobe Animate version 21.0.5 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-06-28	4.3	CVE-2021-28573 MISC
adobe -- connect	Adobe Connect version 11.2.1 (and earlier) is affected by an Improper access control vulnerability that can lead to the elevation of privileges. An attacker with 'Learner' permissions can leverage this scenario to access the list of event participants.	2021-06-28	4	CVE-2021-28579 MISC
adobe -- experience_manager	AEM's Cloud Service offering, as well as versions 6.5.7.0 (and below), 6.4.8.3 (and below) and 6.3.3.8 (and below) are affected by an Improper Access Control vulnerability. An unauthenticated attacker could leverage this vulnerability to	2021-06-28	5	CVE-2021-21083 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cause an application denial-of-service in the context of the current user.			
adobe -- experience_manager	AEM's Cloud Service offering, as well as versions 6.5.7.0 (and below), 6.4.8.3 (and below) and 6.3.3.8 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2021-06-28	4.3	CVE-2021-21084 MISC
apache -- traffic_server	Improper Input Validation vulnerability in HTTP/2 of Apache Traffic Server allows an attacker to DOS the server. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1.	2021-06-30	5	CVE-2021-32567 MISC
apache -- traffic_server	Improper Input Validation vulnerability in HTTP/2 of Apache Traffic Server allows an attacker to DOS the server. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1.	2021-06-30	5	CVE-2021-32566 MISC
auth0 -- nextjs-auth0	The Auth0 Next.js SDK is a library for implementing user authentication in Next.js applications. Versions before and	2021-06-25	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	including `1.4.1` are vulnerable to reflected XSS. An attacker can execute arbitrary code by providing an XSS payload in the `error` query parameter which is then processed by the callback handler as an error message. You are affected by this vulnerability if you are using `@auth0/nextjs-auth0` version `1.4.1` or lower **unless** you are using custom error handling that does not return the error message in an HTML response. Upgrade to version `1.4.1` to resolve. The fix adds basic HTML escaping to the error message and it should not impact your users.			32702 MISC CONFIRM MISC
autodesk -- advance_steel	A maliciously crafted DWG file can be forced to read beyond allocated boundaries when parsing the DWG file. This vulnerability can be exploited to execute arbitrary code.	2021-06-25	6.8	CVE-2021-27040 MISC
autodesk -- advance_steel	A maliciously crafted DWG file can be used to write beyond the allocated buffer while parsing DWG files. This vulnerability can be exploited to execute arbitrary code.	2021-06-25	6.8	CVE-2021-27041 MISC
autodesk -- advance_steel	A maliciously crafted DWG file can be used to write beyond the allocated buffer while parsing DWG files. The vulnerability exists because the application fails to handle a crafted DWG	2021-06-25	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	file, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code.			27042 MISC
autodesk -- advance_steel	An Arbitrary Address Write issue in the Autodesk DWG application can allow a malicious user to leverage the application to write in unexpected paths. In order to exploit this the attacker would need the victim to enable full page heap in the application.	2021-06-25	4.3	CVE-2021-27043 MISC
avaya -- aura_device_services	An arbitrary code execution vulnerability was discovered in Avaya Aura Device Services that may potentially allow a local user to execute specially crafted scripts. Affects 7.0 through 8.1.4.0 versions of Avaya Aura Device Services.	2021-06-25	4.6	CVE-2021-25654 MISC
cisco -- dna_center	A vulnerability in the Cisco Identity Services Engine (ISE) integration feature of the Cisco DNA Center Software could allow an unauthenticated, remote attacker to gain unauthorized access to sensitive data. The vulnerability is due to an incomplete validation of the X.509 certificate used when establishing a connection between DNA Center and an ISE server. An attacker could exploit this vulnerability by supplying a crafted certificate and could then intercept communications between the ISE and DNA Center. A successful exploit could allow the attacker to view and alter sensitive information that	2021-06-29	5.8	CVE-2021-1134 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the ISE maintains about clients that are connected to the network.			
crmeb -- crmeb	SQL Injection vulnerability in Zhong Bang Technology Co., Ltd CRMEB mall system V2.60 and V3.1 via the tablename parameter in SystemDatabackup.php.	2021-06-29	6.5	CVE-2020-21394 MISC
dovecot -- dovecot	The Sieve engine in Dovecot before 2.3.15 allows Uncontrolled Resource Consumption, as demonstrated by a situation with a complex regular expression for the regex extension.	2021-06-28	4	CVE-2020-28200 MISC CONFIRM
dovecot -- dovecot	The submission service in Dovecot before 2.3.15 allows STARTTLS command injection in lib-smtp. Sensitive information can be redirected to an attacker-controlled address.	2021-06-28	5.8	CVE-2021-33515 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
enhancesoft -- osticket	Cross Site Scripting vulnerability in Enhancesoft osTicket before v1.12.6 via the queue-name parameter to include/ajax.search.php.	2021-06-28	4.3	CVE-2020-22608 CONFIRM
enhancesoft -- osticket	Cross Site Scripting (XSS) vulnerability in Enhancesoft osTicket before v1.12.6 via the queue-name parameter in include/class.queue.php.	2021-06-28	4.3	CVE-2020-22609 CONFIRM
fidelissecurity -- deception	User credentials stored in a recoverable format within Fidelis Network and Deception CommandPost. In the event that an attacker gains access to the CommandPost, these values could be decoded and used to login to the application. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.3. This vulnerability has been addressed in version 9.3.3 and subsequent versions.	2021-06-25	5	CVE-2021-35050 CONFIRM
fidelissecurity -- deception	Vulnerability in Fidelis Network and Deception CommandPost enables authenticated command injection through the web interface. The vulnerability could allow a specially crafted HTTP request to execute system commands on the	2021-06-25	6.5	CVE-2021-35049

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CommandPost and return results in an HTTP response in an authenticated session. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability.			CONFIRM
google -- bindiff	An attacker can craft a specific IdaPro *.i64 file that will cause the BinDiff plugin to load an invalid memory offset. This can allow the attacker to control the instruction pointer and execute arbitrary code. It is recommended to upgrade BinDiff 7	2021-06-29	4.6	CVE-2021-22545 MISC
huawei -- ecns280_firmware	There is an XXE injection vulnerability in eCNS280 V100R005C00 and V100R005C10. A module does not perform the strict operation to the input XML message. Attacker can send specific message to exploit this vulnerability, leading to the module denial of service.	2021-06-29	5	CVE-2021-22338 MISC
huawei -- emui	There is an Information Disclosure Vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause out-of-bounds read.	2021-06-30	6.4	CVE-2021-22354 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- ips_module_firmware	There is a memory leak vulnerability in Huawei products. A resource management weakness exists in a module. Attackers with high privilege can exploit this vulnerability by performing some operations. This can lead to memory leak. Affected product versions include:IPS Module V500R005C00SPC100,V500R005C00SPC200;NGFW Module V500R005C00SPC100,V500R005C00SPC200;NIP6300 V500R005C00SPC100,V500R005C10SPC200;NIP6600 V500R005C00SPC100,V500R005C00SPC200;Secospace USG6300 V500R005C00SPC100,V500R005C00SPC200;Secospace USG6500 V500R005C00SPC100,V500R005C10SPC200;Secospace USG6600 V500R005C00SPC100,V500R005C00SPC200.	2021-06-29	4	CVE-2021-22341 MISC
ibm -- business_automation_workflow	IBM Business Automation Workflow 19.0.03 and 20.0 and IBM Cloud Pak for Automation 20.0.3-IF002 and 21.0.1 are 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: 203029.	2021-06-28	4.3	CVE-2021-29775 CONFIRM CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 4.0.0.4 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196212.	2021-06-28	5	CVE-2021-20413 XF CONFIRM
ibm -- planning_analytics	IBM Planning Analytics 2.0 could be vulnerable to cross-site request forgery (CSRF) which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 198241.	2021-06-29	4.3	CVE-2021-20580 CONFIRM XF
ibm -- security_identity_manager_adapter	IBM Security Identity Manager Adapters 6.0 and 7.0 are vulnerable to a heap-based buffer overflow, caused by improper bounds checking. A remote authenticated attacker could overflow the and cause the server to crash. IBM X-Force ID: 199249.	2021-06-28	4	CVE-2021-20573 CONFIRM XF
ibm -- security_identity_manager_adapter	IBM Security Identity Manager Adapters 6.0 and 7.0 are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A remote authenticated attacker could	2021-06-28	4	CVE-2021-20572

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	overflow the and cause the server to crash. IBM X-Force ID: 199247.			CONFIRM XF
ibm -- security_identity_manager_adapter	IBM Security Identity Manager Adapters 6.0 and 7.0 are vulnerable to a heap based buffer overflow, caused by improper bounds. An authenticared user could overflow the buffer and cause the service to crash. IBM X-Force ID: 197882.	2021-06-28	4	CVE-2021-20494 CONFIRM XF
ibm -- security_verify	IBM Security Verify (IBM Security Verify Privilege Vault 10.9.66) could disclose sensitive information through an HTTP GET request by a privileged user due to improper input validation.. IBM X-Force ID: 199396.	2021-06-25	4	CVE-2021-20583 XF CONFIRM
ibm -- security_verify	IBM Security Verify (IBM Security Verify Privilege Vault 10.9.66) is vulnerable to link injection. By persuading a victim to click on a specially-crafted URL link, a remote attacker could exploit this vulnerability to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking	2021-06-25	5.8	CVE-2021-29676 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_privilege_manager	IBM Security Sevret Server (IBM Security Verify Privilege Manager 10.8.2) could allow a local user to execute code due to improper integrity checks. IBM X-Force ID: 184919.	2021-06-25	4.6	CVE-2020-4610 XF CONFIRM
ibm -- security_verify_privilege_manager	IBM Security Sevret Server (IBM Security Verify Privilege Manager 10.8.2) is vulnerable to a buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and execute arbitrary code on the system or cause the system to crash. IBM X-Force ID: 184917.	2021-06-25	4.6	CVE-2020-4609 XF CONFIRM
imagemagick -- imagemagick	ImageMagick 7.0.11-14 has a memory leak in AcquireSemaphoreMemory in semaphore.c and AcquireMagickMemory in memory.c.	2021-06-25	5	CVE-2021-34183 CONFIRM
infoblox -- nios	Infoblox NIOS before 8.5.2 allows entity expansion during an XML upload operation, a related issue to CVE-2003-1564.	2021-06-28	4	CVE-2020-15303

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
ipfire -- ipfire	Cross Site Scripting (XSS) vulnerabilty in IPFire 2.23 via the IPfire web UI in the mail.cgi.	2021-06-28	4.3	CVE-2020-21142 MISC
istio -- istio	Istio before 1.9.6 and 1.10.x before 1.10.2 has Incorrect Access Control.	2021-06-29	6.5	CVE-2021-34824 MISC MISC
limesurvey -- limesurvey	Cross Site Scripting vulnerabilty in LimeSurvey 4.1.11+200316 via the (1) name and (2) description parameters in application/controllers/admin/PermissiontemplatesController.php.	2021-06-28	4.3	CVE-2020-22607 CONFIRM
machform -- machform	Machform prior to version 16 is vulnerable to stored cross-site scripting due to insufficient sanitization of file attachments uploaded with forms through upload.php.	2021-06-29	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				20103 MISC
machform -- machform	Machform prior to version 16 is vulnerable to an open redirect in Safari_init.php due to an improperly sanitized 'ref' parameter.	2021-06-29	5.8	CVE-2021-20105 MISC
machform -- machform	Machform prior to version 16 is vulnerable to HTTP host header injection due to improperly validated host headers. This could cause a victim to receive malformed content.	2021-06-29	5.8	CVE-2021-20101 MISC
machform -- machform	Machform prior to version 16 is vulnerable to cross-site request forgery due to a lack of CSRF tokens in place.	2021-06-29	6.8	CVE-2021-20102 MISC
machform -- machform	Machform prior to version 16 is vulnerable to unauthenticated remote code execution due to insufficient sanitization of file attachments uploaded with forms through upload.php.	2021-06-29	6.8	CVE-2021-20104 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
magento -- magento	Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by an Improper Authorization vulnerability via the 'Create Customer' endpoint. Successful exploitation could lead to unauthorized modification of customer data by an unauthenticated attacker. Access to the admin console is required for successful exploitation.	2021-06-28	6.4	CVE-2021-28563 MISC
mermaid_project -- mermaid	Mermaid before 8.11.0 allows XSS when the antiscript feature is used.	2021-06-27	4.3	CVE-2021-35513 MISC MISC MISC
miniaudio_project -- miniaudio	Miniaudio 0.10.35 has an integer-based buffer overflow caused by an out-of-bounds left shift in drwav_bytes_to_u32 in miniaudio.h	2021-06-25	6.8	CVE-2021-34185 CONFIRM
miraheze -- globalnewfiles	GlobalNewFiles is a mediawiki extension. All existing versions of GlobalNewFiles are affected by an uncontrolled resource consumption vulnerability. A large amount of page moves within a short space of time could overwhelm Database servers	2021-06-28	4	CVE-2021-32722 CONF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	due to improper handling of load balancing and a lack of an appropriate index. No patches are currently available. As a workaround, one may avoid use of the extension unless additional rate limit at the MediaWiki level or via PoolCounter / MySQL is enabled.			IRM MISC
nvidia -- geforce_experience	NVIDIA GeForce Experience, all versions prior to 3.23, contains a vulnerability where, if a user clicks on a maliciously formatted link that opens the GeForce Experience login page in a new browser tab instead of the GeForce Experience application and enters their login information, the malicious site can get access to the token of the user login session. Such an attack may lead to these targeted users' data being accessed, altered, or lost.	2021-06-25	6.8	CVE-2021-1073 CONF IRM
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. 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 parsing of CGM files. 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 buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13679.	2021-06-29	6.8	CVE-2021-31514 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 parsing of CGM files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12653.	2021-06-29	6.8	CVE-2021-31507 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to disclose sensitive information on affected installations of OpenText Brava! Desktop Build 16.6.4.55. 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 parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13674.	2021-06-29	4.3	CVE-2021-31506 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this	2021-06-29	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. 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 buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13306.			31508 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. 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 parsing of BMP files. 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 buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13678.	2021-06-29	6.8	CVE-2021-31513 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. 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 parsing of TIF files. The issue results from the lack of proper validation	2021-06-29	6.8	CVE-2021-31512 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13677.			
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. 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 parsing of DXF files. 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 buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13309.	2021-06-29	6.8	CVE-2021-31509 MISC
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. 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 parsing of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability	2021-06-29	6.8	CVE-2021-31510 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to execute code in the context of the current process. Was ZDI-CAN-13675.			
opentext -- brava\!_desktop	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. 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 parsing of PDF files. 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 buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13676.	2021-06-29	6.8	CVE-2021-31511 MISC
oracle -- glassfish_server	** UNSUPPORTED WHEN ASSIGNED ** Oracle GlassFish Server 3.1.2.18 and below allows /common/logViewer/logViewer.jsf XSS. A malicious user can cause an administrator user to supply dangerous content to the vulnerable page, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to victims. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2021-06-25	4.3	CVE-2021-3314 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phoenixcontact -- config\+	Phoenix Contact Classic Automation Worx Software Suite in Version 1.87 and below is affected by a remote code execution vulnerability. Manipulated PC Worx or Config+ projects could lead to a remote code execution when unallocated memory is freed because of incompletely initialized data. The attacker needs to get access to an original bus configuration file (*.bcp) to be able to manipulate data inside. After manipulation the attacker needs to exchange the original file by the manipulated one on the application programming workstation. Availability, integrity, or confidentiality of an application programming workstation might be compromised by attacks using these vulnerabilities. Automated systems in operation which were programmed with one of the above-mentioned products are not affected.	2021-06-25	5.1	CVE-2021-33542 CONFIRM
phoenixcontact -- fl_comserver_uni_232\/422\/485_firmware	In Phoenix Contact FL COMSERVER UNI in versions < 2.40 a invalid Modbus exception response can lead to a temporary denial of service.	2021-06-25	5	CVE-2021-21002 CONFIRM
phoenixcontact -- fl_switch_smcs_16tx_firmware	In Phoenix Contact FL SWITCH SMCS series products in multiple versions fragmented TCP-Packets may cause a Denial of Service of Web-, SNMP- and ICMP-Echo services. The switching functionality of the device is not affected.	2021-06-25	5	CVE-2021-21003

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
phoenixcontact -- fl_switch_smcs_16tx_firmware	In Phoenix Contact FL SWITCH SMCS series products in multiple versions an attacker may insert malicious code via LLDP frames into the web-based management which could then be executed by the client.	2021-06-25	4.3	CVE-2021-21004 CONFIRM
postsrsd_project -- postsrsd	PostSRSd before 1.11 allows a denial of service (subprocess hang) if Postfix sends certain long data fields such as multiple concatenated email addresses. NOTE: the PostSRSd maintainer acknowledges "theoretically, this error should never occur ... I'm not sure if there's a reliable way to trigger this condition by an external attacker, but it is a security bug in PostSRSd nevertheless."	2021-06-28	5	CVE-2021-35525 MISC MISC MISC
poweriso -- poweriso	A memory corruption vulnerability exists in the DMG File Format Handler functionality of PowerISO 7.9. A specially crafted DMG file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability. The vendor fixed it in a bug-release of the current version.	2021-06-29	6.8	CVE-2021-21871 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
prismjs -- prism	Prism is a syntax highlighting library. Some languages before 1.24.0 are vulnerable to Regular Expression Denial of Service (ReDoS). When Prism is used to highlight untrusted (user-given) text, an attacker can craft a string that will take a very very long time to highlight. This problem has been fixed in Prism v1.24. As a workaround, do not use ASCIIDoc or ERB to highlight untrusted text. Other languages are not affected and can be used to highlight untrusted text.	2021-06-28	4.3	CVE-2021-32723 CONFIRM MISC MISC
python -- urllib3	An issue was discovered in urllib3 before 1.26.5. When provided with a URL containing many @ characters in the authority component, the authority regular expression exhibits catastrophic backtracking, causing a denial of service if a URL were passed as a parameter or redirected to via an HTTP redirect.	2021-06-29	5	CVE-2021-33503 CONFIRM CONFIRM
shopex -- ecshop	Cross Site Scripting (XSS) vulnerability in ECShop 4.0 due to security filtering issues, in the user.php file, we can use the html entity encoding to bypass the security policy of the safety.php file, triggering the xss vulnerability.	2021-06-28	4.3	CVE-2020-20640 MISC
siemens -- sinamics_sl150_firmware	The Telnet service of the SIMATIC HMI Comfort Panels system component in affected products does not require	2021-06-28	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authentication, which may allow a remote attacker to gain access to the device if the service is enabled. Telnet is disabled by default on the SINAMICS Medium Voltage Products (SINAMICS SL150: All versions, SINAMICS SM150: All versions, SINAMICS SM150i: All versions).			31337 MISC
sylius -- sylius	Sylius is an Open Source eCommerce platform on top of Symfony. In versions of Sylius prior to 1.9.5 and 1.10.0-RC.1, part of the details (order ID, order number, items total, and token value) of all placed orders were exposed to unauthorized users. If exploited properly, a few additional information like the number of items in the cart and the date of the shipping may be fetched as well. This data seems to not be crucial nor is personal data, however, could be used for sociotechnical attacks or may expose a few details about shop condition to the third parties. The data possible to aggregate are the number of processed orders or their value in the moment of time. The problem has been patched at Sylius 1.9.5 and 1.10.0-RC.1. There are a few workarounds for the vulnerability. The first possible solution is to hide the problematic endpoints behind the firewall from not logged in users. This would put only the order list under the firewall and allow only authorized users to access it. Once a user is authorized, it will have access to theirs orders only. The second possible solution is to decorate the `\Sylius\Bundle\ApiBundle\Doctrine\QueryCollectionExtension	2021-06-28	5	CVE-2021-32720 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	\OrdersByLoggedInUserExtension` and throw `Symfony\Component\Security\Core\Exception\AccessDeniedException` if the class is executed for unauthorized user.			
tenable -- nessus	Nessus Agent 8.2.4 and earlier for Windows were found to contain multiple local privilege escalation vulnerabilities which could allow an authenticated, local administrator to run specific Windows executables as the Nessus host. This is different than CVE-2021-20099.	2021-06-28	4.6	CVE-2021-20100 MISC
tenable -- nessus	Nessus Agent 8.2.4 and earlier for Windows were found to contain multiple local privilege escalation vulnerabilities which could allow an authenticated, local administrator to run specific Windows executables as the Nessus host. This is different than CVE-2021-20100.	2021-06-28	4.6	CVE-2021-20099 MISC
umbraco -- umbraco_cms	Umbraco CMS before 7.15.7 is vulnerable to Open Redirection due to insufficient url sanitization on booting.aspx.	2021-06-28	5.8	CVE-2021-34254 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
unidocs -- ezpdf_editor	A memory corruption vulnerability exists when ezPDF improperly handles the parameter. This vulnerability exists due to insufficient validation of the parameter.	2021-06-29	6.5	CVE-2020-7870 MISC
vector35 -- binary_ninja	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Vector 35 Binary Ninja 2.3.2660 (Build ID 88f343c3). 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 parsing of BNDB files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13670.	2021-06-29	6.8	CVE-2021-31516 MISC MISC
vector35 -- binary_ninja	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Vector 35 Binary Ninja 2.3.2660 (Build ID 88f343c3). 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 parsing of BNDB files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage	2021-06-29	6.8	CVE-2021-31515 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13668.			
vmware -- spring_security	Spring Security versions 5.5.x prior to 5.5.1, 5.4.x prior to 5.4.7, 5.3.x prior to 5.3.10 and 5.2.x prior to 5.2.11 are susceptible to a Denial-of-Service (DoS) attack via the initiation of the Authorization Request in an OAuth 2.0 Client Web and WebFlux application. A malicious user or attacker can send multiple requests initiating the Authorization Request for the Authorization Code Grant, which has the potential of exhausting system resources using a single session or multiple sessions.	2021-06-29	5	CVE-2021-22119 MISC
webport_cms_project -- webport_cms	Directory Traversal vulnerability in Webport CMS 1.19.10.17121 via the file parameter to file/download.	2021-06-28	5	CVE-2020-23715 MISC
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable denial-of-service vulnerability exists in ServiceAgent functionality. A specially crafted packet can cause an integer underflow, triggering a large memcpy that will access unmapped or out-of-bounds memory. An attacker can send this packet while unauthenticated to trigger this vulnerability.	2021-06-25	5	CVE-2021-33536 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable format string vulnerability exists in the iw_console conio_writestr functionality. A specially crafted time server entry can cause an overflow of the time server buffer, resulting in remote code execution. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.	2021-06-25	6.5	CVE-2021-33535 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions the usage of hard-coded cryptographic keys within the service agent binary allows for the decryption of captured traffic across the network from or to the device.	2021-06-25	5	CVE-2021-33529 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable authentication bypass vulnerability exists in the hostname processing. A specially configured device hostname can cause the device to interpret selected remote traffic as local traffic, resulting in a bypass of web authentication. An attacker can send authenticated SNMP requests to trigger this vulnerability.	2021-06-25	6.5	CVE-2021-33539 CONFIRM
weidmueller -- ie-wl-bl-ap-cl-eu_firmware	In Weidmueller Industrial WLAN devices in multiple versions an exploitable remote code execution vulnerability exists in the	2021-06-25	6.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	iw_webs configuration parsing functionality. A specially crafted user name entry can cause an overflow of an error message buffer, resulting in remote code execution. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.			33537 CONFIRM
zammad -- zammad	Cross Site Scripting (XSS) in Zammad 1.0.x up to 4.0.0 allows remote attackers to execute arbitrary web script or HTML via multiple models that contain a 'note' field to store additional information.	2021-06-28	4.3	CVE-2021-35298 CONFIRM
zammad -- zammad	Text injection/Content Spoofing in 404 page in Zammad 1.0.x up to 4.0.0 could allow remote attackers to manipulate users into visiting the attackers' page.	2021-06-28	4.3	CVE-2021-35300 CONFIRM
zammad -- zammad	Cross Site Scripting (XSS) in Zammad 1.0.x up to 4.0.0 allows remote attackers to execute arbitrary web script or HTML via the User Avatar attribute.	2021-06-28	4.3	CVE-2021-35303 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zammad -- zammad	Incorrect Access Control for linked Tickets in Zammad 1.0.x up to 4.0.0 allows remote attackers to obtain sensitive information.	2021-06-28	5	CVE-2021-35302 CONFIRM
zammad -- zammad	Incorrect Access Control in Zammad 1.0.x up to 4.0.0 allows remote attackers to obtain sensitive information via the Ticket Article detail view.	2021-06-28	5	CVE-2021-35301 CONFIRM
zammad -- zammad	Incorrect Access Control in Zammad 1.0.x up to 4.0.0 allows attackers to obtain sensitive information via email connection configuration probing.	2021-06-28	5	CVE-2021-35299 CONFIRM
zohocorp -- manageengine_servicedesk_plus	Zoho ManageEngine ServiceDesk Plus MSP before 10521 allows an attacker to access internal data.	2021-06-29	5	CVE-2021-31160 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zohocorp -- manageengine_servicedesk_plus_msp	Zoho ManageEngine ServiceDesk Plus MSP before 10522 is vulnerable to Information Disclosure.	2021-06-29	5	CVE-2021-31530 CONFIRM
zrlog -- zrlog	Cross Site Scripting vulnerability in ZrLog 2.1.0 via the (1) userName and (2) email parameters in post/addComment.	2021-06-29	4.3	CVE-2020-18066 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- photoshop_elements	Adobe Photoshop Elements version 5.2 (and earlier) is affected by an insecure temporary file creation vulnerability. An unauthenticated attacker could leverage this vulnerability to call functions against the installer to perform high privileged	2021-06-28	2.1	CVE-2021-28597 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	actions. Exploitation of this issue does not require user interaction.			
adobe -- premiere_elements	Adobe Premiere Elements version 5.2 (and earlier) is affected by an insecure temporary file creation vulnerability. An unauthenticated attacker could leverage this vulnerability to call functions against the installer to perform high privileged actions. Exploitation of this issue does not require user interaction.	2021-06-28	2.1	CVE-2021-28623 MISC
bluetooth -- bluetooth_core_specification	Unencrypted Bluetooth Low Energy baseband links in Bluetooth Core Specifications 4.0 through 5.2 may permit an adjacent device to inject a crafted packet during the receive window of the listening device before the transmitting device initiates its packet transmission to achieve full MITM status without terminating the link. When applied against devices establishing or using encrypted links, crafted packets may be used to terminate an existing link, but will not compromise the confidentiality or integrity of the link.	2021-06-25	2.9	CVE-2021-31615 MISC MISC
cabrerahector -- popular_posts	Cross-site scripting vulnerability in WordPress Popular Posts 5.3.2 and earlier allows a remote	2021-06-28	3.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated attacker to inject an arbitrary script via unspecified vectors.			20746 MISC MISC MISC MISC
dovecot -- dovecot	Dovecot before 2.3.15 allows ../ Path Traversal. An attacker with access to the local filesystem can trick OAuth2 authentication into using an HS256 validation key from an attacker-controlled location. This occurs during use of local JWT validation with the posix fs driver.	2021-06-28	2.1	CVE-2021-29157 MISC CONFIRM
ibm -- aix	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a local user that is in the with elevated group privileges to cause a denial of service due to a vulnerability in the lpd daemon. IBM X-Force ID: 200255.	2021-06-28	2.1	CVE-2021-29693 XF CONFIRM
ibm -- business_automation_workflow	IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.5 and 8.6 could allow an authenticated user to obtain sensitive information about another user under nondefault configurations. IBM X-Force ID: 201779.	2021-06-28	3.5	CVE-2021-29751 CONFIRM CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- planning_analytics	IBM Planning Analytics 2.0 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: 196949.	2021-06-29	3.5	CVE-2021-20477 CONFIRM XF
ibm -- security_verify	IBM Security Verify (IBM Security Verify Privilege Vault 10.9.66) 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.	2021-06-25	3.5	CVE-2021-29677 CONFIRM XF
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.8 could allow a local user to cause a denial of service due to insecure file permission settings. IBM X-Force ID: 197791.	2021-06-29	2.1	CVE-2021-20490 CONFIRM XF
limesurvey -- limesurvey	Cross Site Scripting (XSS) vulneraiblity in LimeSurvey 4.2.5 on textbox via the Notifications & data feature.	2021-06-28	3.5	CVE-2020-23710 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
magento -- magento	Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by a DOM-based Cross-Site Scripting vulnerability on mage-messages cookies. Successful exploitation could lead to arbitrary JavaScript execution by an unauthenticated attacker. User interaction is required for successful exploitation.	2021-06-28	3.5	CVE-2021-28556 MISC
pandorafms -- pandora_fms	PandoraFMS <=7.54 allows Stored XSS by placing a payload in the name field of a visual console. When a user or an administrator visits the console, the XSS payload will be executed.	2021-06-25	3.5	CVE-2021-35501 MISC
plone -- plone	In Plone 5.0 through 5.2.4, Editors are vulnerable to XSS in the folder contents view, if a Contributor has created a folder with a SCRIPT tag in the description field.	2021-06-30	3.5	CVE-2021-35959 MISC MLIST
sas -- environment_manager	SAS Environment Manager 2.5 allows XSS through the Name field when creating/editing a server. The XSS will prompt when editing the Configuration Properties.	2021-06-25	3.5	CVE-2021-35475 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sick -- visionary-s_cx_firmware	SICK Visionary-S CX up version 5.21.2.29154R are vulnerable to an Inadequate Encryption Strength vulnerability concerning the internal SSH interface solely used by SICK for recovering returned devices. The use of weak ciphers make it easier for an attacker to break the security that protects information transmitted from the client to the SSH server, assuming the attacker has access to the network on which the device is connected. This can increase the risk that encryption will be compromised, leading to the exposure of sensitive user information and man-in-the-middle attacks.	2021-06-28	3.5	CVE-2021-32496 MISC
tripplite -- su2200rtxl2ua_firmware	A stored cross-site scripting (XSS) vulnerability was discovered in /Forms/device_vars_1 on TrippLite SU2200RTXL2Ua with firmware version 12.04.0055. This vulnerability allows authenticated attackers to obtain other users' information via a crafted POST request.	2021-06-25	3.5	CVE-2020-26801 MISC MISC MISC
vmware -- rabbitmq	RabbitMQ is a multi-protocol messaging broker. In rabbitmq-server prior to version 3.8.17, a new user being added via management UI could lead to the user's bane being rendered in a confirmation message without proper `<script>` tag sanitization, potentially allowing for JavaScript code execution in the context of the page. In order for this to	2021-06-28	3.5	CVE-2021-32718 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	occur, the user must be signed in and have elevated permissions (other user management). The vulnerability is patched in RabbitMQ 3.8.17. As a workaround, disable `rabbitmq_management` plugin and use CLI tools for management operations and Prometheus and Grafana for metrics and monitoring.			
vmware -- rabbitmq	RabbitMQ is a multi-protocol messaging broker. In rabbitmq-server prior to version 3.8.18, when a federation link was displayed in the RabbitMQ management UI via the `rabbitmq_federation_management` plugin, its consumer tag was rendered without proper <script> tag sanitization. This potentially allows for JavaScript code execution in the context of the page. The user must be signed in and have elevated permissions (manage federation upstreams and policies) for this to occur. The vulnerability is patched in RabbitMQ 3.8.18. As a workaround, disable the `rabbitmq_federation_management` plugin and use [CLI tools](https://www.rabbitmq.com/cli.html) instead.	2021-06-28	3.5	CVE-2021-32719 MISC CONFIRM MISC