Vulnerability Summary for the Week of May 24, 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
aioseo -- all_in_one_seo	The All in One SEO – Best WordPress SEO Plugin – Easily Improve Your SEO Rankings before 4.1.0.2 enables authenticated users with "aioseo_tools_settings" privilege (most of the time admin) to execute arbitrary code on the underlying host. Users can restore plugin's configuration by uploading a backup .ini file in the section "Tool > Import/Export". However, the plugin attempts to unserialize values of the .ini file. Moreover, the plugin embeds	2021-05-24	9	CVE-2021-24307 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Monolog library which can be used to craft a gadget chain and thus trigger system command execution.			
cisco -- dna_spaces\	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. These vulnerabilities are due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities by leveraging the insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin and execute arbitrary commands on the underlying operating system as root.	2021-05-22	7.2	CVE-2021-1558 CISCO
cisco -- dna_spaces\	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. These vulnerabilities are	2021-05-22	7.2	CVE-2021-1557 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities by leveraging the insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin and execute arbitrary commands on the underlying operating system as root.			
cisco -- dna_spaces\	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, remote attacker to perform a command injection attack on an affected device. These vulnerabilities are due to insufficient input sanitization when executing affected commands. A high-privileged attacker could exploit these vulnerabilities on a Cisco DNA Spaces Connector by injecting crafted input during command execution. A successful exploit could allow the attacker to execute arbitrary commands as root within the Connector docker container.	2021-05-22	9	CVE-2021-1560 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- dna_spaces\	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, remote attacker to perform a command injection attack on an affected device. These vulnerabilities are due to insufficient input sanitization when executing affected commands. A high-privileged attacker could exploit these vulnerabilities on a Cisco DNA Spaces Connector by injecting crafted input during command execution. A successful exploit could allow the attacker to execute arbitrary commands as root within the Connector docker container.	2021-05-22	9	CVE-2021-1559 CISCO
cisco -- evolved_programmable_network_manager	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Evolved Programmable Network (EPN) Manager could allow an authenticated, remote attacker to execute arbitrary commands on an affected system. The vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP	2021-05-22	9	CVE-2021-1487 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	requests to the interface. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system (OS) with the permissions of a special non-root user. In this way, an attacker could take control of the affected system, which would allow them to obtain and alter sensitive data. The attacker could also affect the devices that are managed by the affected system by pushing arbitrary configuration files, retrieving device credentials and confidential information, and ultimately undermining the stability of the devices, causing a denial of service (DoS) condition.			
cisco -- modeling_labs	A vulnerability in the web UI of Cisco Modeling Labs could allow an authenticated, remote attacker to execute arbitrary commands with the privileges of the web application on the underlying operating system of an affected Cisco Modeling Labs server. This vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker	2021-05-22	9	CVE-2021-1531 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could exploit this vulnerability by sending a crafted HTTP request to an affected server. A successful exploit could allow the attacker to execute arbitrary commands with the privileges of the web application, virl2, on the underlying operating system of the affected server. To exploit this vulnerability, the attacker must have valid user credentials on the web UI.			
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the	2021-05-22	9	CVE-2021-1550 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.			
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1555 CISCO
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series	2021-05-22	9	CVE-2021-1554 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.			
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted	2021-05-22	9	CVE-2021-1553 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.			
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities,	2021-05-22	9	CVE-2021-1552 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the attacker must have valid administrative credentials for the device.			
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1551 CISCO
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an	2021-05-22	9	CVE-2021-1548 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.			
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based	2021-05-22	9	CVE-2021-1549 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.			
cisco -- wap125_firmware	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	2021-05-22	9	CVE-2021-1547 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codesys -- v2_runtime_system_sp	CODESYS V2 runtime system SP before 2.4.7.55 has a Stack-based Buffer Overflow.	2021-05-25	7.5	CVE-2021-30188 MISC MISC
codesys -- v2_web_server	CODESYS V2 Web-Server before 1.1.9.20 has a Stack-based Buffer Overflow.	2021-05-25	7.5	CVE-2021-30189 MISC MISC
codesys -- v2_web_server	CODESYS V2 Web-Server before 1.1.9.20 has Improper Access Control.	2021-05-25	7.5	CVE-2021-30190 MISC MISC
codesys -- v2_web_server	CODESYS V2 Web-Server before 1.1.9.20 has an Improperly Implemented Security Check.	2021-05-25	7.5	CVE-2021-30192 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codesys -- v2_web_server	CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Write.	2021-05-25	7.5	CVE-2021-30193 MISC MISC
college_management_system_project -- college_management_system	Projectsworlds College Management System Php 1.0 is vulnerable to SQL injection issues over multiple parameters.	2021-05-24	7.5	CVE-2020-25409 MISC MISC
deep-defaults_project -- deep-defaults	Prototype pollution vulnerability in 'deep-defaults' versions 1.0.0 through 1.0.5 allows attacker to cause a denial of service and may lead to remote code execution.	2021-05-25	7.5	CVE-2021-25944 MISC
eyesofnetwork -- eyesofnetwork	EyesOfNetwork eonweb through 5.3-11 allows Remote Command Execution (by authenticated users) via shell metacharacters in the nagios_path parameter to lilac/export.php, as demonstrated by %26%26+curl to insert an "&& curl" substring for the shell.	2021-05-24	9	CVE-2021-33525 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_guardium	IBM Security Guardium 11.2 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 195766.	2021-05-24	9	CVE-2021-20385 CONFIRM XF
ibm -- security_guardium	IBM Security Guardium 11.2 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 199184.	2021-05-24	9	CVE-2021-20557 XF CONFIRM
ibm -- security_guardium	IBM Security Guardium 11.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 196313.	2021-05-24	7.5	CVE-2021-20426 CONFIRM XF
linux -- linux_kernel	This vulnerability allows local attackers to escalate privileges on affected	2021-05-21	7.2	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	installations of Linux Kernel 5.11.15. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of eBPF programs. The issue results from the lack of proper validation of user-supplied eBPF programs prior to executing them. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel. Was ZDI-CAN-13661.			31440 MISC MISC
nagios -- fusion	Insufficient Verification of Data Authenticity in Nagios Fusion 4.1.8 and earlier and Nagios XI 5.7.5 and earlier allows for Escalation of Privileges or Code Execution as root via vectors related to an untrusted update package to upgrade_to_latest.sh.	2021-05-24	10	CVE-2020-28900 MISC MISC MISC
nagios -- fusion	Command Injection in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation to nagios.	2021-05-24	7.5	CVE-2020-28908 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
nagios -- fusion	Command Injection in Nagios Fusion 4.1.8 and earlier allows Privilege Escalation from apache to root in cmd_subsys.php.	2021-05-24	10	CVE-2020-28902 MISC MISC MISC
nagios -- fusion	Incorrect SSL certificate validation in Nagios Fusion 4.1.8 and earlier allows for Escalation of Privileges or Code Execution as root via vectors related to download of an untrusted update package in upgrade_to_latest.sh.	2021-05-24	10	CVE-2020-28907 MISC MISC MISC
nagios -- fusion	Incorrect File Permissions in Nagios XI 5.7.5 and earlier and Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation to root. Low-privileged users are able to modify files that are included (aka sourced) by scripts executed by root.	2021-05-24	9	CVE-2020-28906 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nagios -- fusion	Command Injection in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation or Code Execution as root via vectors related to corrupt component installation in cmd_subsys.php.	2021-05-24	10	CVE-2020-28901 MISC MISC MISC
nagios -- fusion	Incorrect File Permissions in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation to root via modification of scripts. Low-privileges users are able to modify files that can be executed by sudo.	2021-05-24	9	CVE-2020-28909 MISC MISC MISC
nagios -- fusion	Execution with Unnecessary Privileges in Nagios Fusion 4.1.8 and earlier allows for Privilege Escalation as nagios via installation of a malicious component containing PHP code.	2021-05-24	7.5	CVE-2020-28904 MISC MISC MISC
nagios -- nagios_xi	Creation of a Temporary Directory with Insecure Permissions in Nagios XI 5.7.5 and earlier allows for Privilege Escalation	2021-05-24	10	CVE-2020-28910 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	via creation of symlinks, which are mishandled in getprofile.sh.			MISC MISC
nconf-toml_project -- nconf-toml	Prototype pollution vulnerability in `nconf-toml` versions 0.0.1 through 0.0.2 allows an attacker to cause a denial of service and may lead to remote code execution.	2021-05-25	7.5	CVE-2021-25946 MISC MISC
netgear -- gc108p_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before	2021-05-21	10	CVE-2021-33514 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3.			
plone -- plone	Plone through 5.2.4 allows remote authenticated managers to perform disk I/O via crafted keyword arguments to the ReStructuredText transform in a Python script.	2021-05-21	8.5	CVE-2021-33509 MISC MLIST
re-logic -- terraria	Re-Logic Terraria before 1.4.2.3 performs Insecure Deserialization.	2021-05-24	7.5	CVE-2021-32075 MISC MISC MISC MISC
ronomon -- opened	The @ronomon/opened library before 1.5.2 is vulnerable to a command injection vulnerability which would allow a remote attacker to execute commands on the system if the library was used with untrusted input.	2021-05-24	10	CVE-2021-29300 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
solarwinds -- network_performance_monitor	This vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Network Performance Monitor 2020.2.1. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SolarWinds.Serialization library. 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-12213.	2021-05-21	10	CVE-2021-31474 MISC MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. A heap-based buffer overflow in function WebPDecodeRGBInto is possible due to an invalid check for buffer size. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	7.5	CVE-2020-36328 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. A use-after-free was found	2021-05-21	7.5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	due to a thread being killed too early. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.			36329 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. An unitialized variable is used in function ReadSymbol. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	7.5	CVE-2018-25014 MISC
webmproject -- libwebp	A flaw was found in libwebp in versions before 1.0.1. A heap-based buffer overflow was found in PutLE16(). The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-21	7.5	CVE-2018-25011 MISC
zephyrproject -- zephyr	Possible read out of bounds in dns read. Zephyr versions >= 1.14.2, >= 2.3.0 contain Out-of-bounds Read (CWE-125). For more information, see https://github.com/zephyrproject-	2021-05-25	7.5	CVE-2020-13601 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	rtos/zephyr/security/advisories/GHSA-mm57-9hqw-qh44			
zephyrproject -- zephyr	Improper Input Frame Validation in ieee802154 Processing. Zephyr versions >= v1.14.2, >= v2.2.0 contain Stack-based Buffer Overflow (CWE-121), Heap-based Buffer Overflow (CWE-122). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-3gvq-h42f-v3c7	2021-05-25	7.5	CVE-2020-10064 MISC
zzcms -- zzcms	An issue was discovered in zzcms 2019. SQL Injection exists in user/ztconfig.php via the daohang or img POST parameter.	2021-05-24	7.5	CVE-2019-12348 MISC

Medium and Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autoptimize -- autoptimize	The Autoptimize WordPress plugin before 2.8.4 was missing proper escaping and sanitisation in some of its settings, allowing high privilege users to set XSS payloads in them, leading to stored Cross-Site Scripting issues	2021-05-24	3.5	CVE-2021-24332 CONFIRM MISC
bluemedicinelabs -- hotjar_connecticator	The Hotjar Connecticator WordPress plugin through 1.1.1 is vulnerable to Stored Cross-Site Scripting (XSS) in the 'hotjar script' textarea. The request did include a CSRF nonce that was properly verified by the server and this vulnerability could only be exploited by administrator users.	2021-05-24	3.5	CVE-2021-24301 CONFIRM
centreon -- centreon	Centreon version 20.10.2 is affected by a cross-site scripting (XSS) vulnerability. The dep_description (Dependency Description) and dep_name (Dependency Name) parameters are vulnerable to stored XSS. A user has to log in and go to the Configuration > Notifications > Hosts page.	2021-05-26	3.5	CVE-2021-27676 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- evolved_programmable_network_manager	A vulnerability in the restricted shell of Cisco Evolved Programmable Network (EPN) Manager, Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to identify directories and write arbitrary files to the file system. This vulnerability is due to improper validation of parameters that are sent to a CLI command within the restricted shell. An attacker could exploit this vulnerability by logging in to the device and issuing certain CLI commands. A successful exploit could allow the attacker to identify file directories on the affected device and write arbitrary files to the file system on the affected device. To exploit this vulnerability, the attacker must be an authenticated shell user.	2021-05-22	3.6	CVE-2021-1306 CISCO
gowebsolutions -- wp_customer_reviews	The WP Customer Reviews WordPress plugin before 3.5.6 did not sanitise some of its settings, allowing high privilege users such as administrators to set XSS payloads in them which will	2021-05-24	3.5	CVE-2021-24296 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	then be triggered in pages where reviews are enabled			
ibm -- security_guardium	IBM Security Guardium 11.2 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 195770.	2021-05-24	2.1	CVE-2021-20389 CONFIRM XF
keystonejs -- keystone-5	Keystone 5 is an open source CMS platform to build Node.js applications. This security advisory relates to a newly discovered capability in our query infrastructure to directly or indirectly expose the values of private fields, bypassing the configured access control. This is an access control related oracle attack in that the attack method guides an attacker during their attempt to reveal information they do not have access to. The complexity of completing the attack is limited by some length-dependent behaviors and the fidelity of the exposed information. Under some circumstances, field values or field value meta data can be determined, despite the field or list	2021-05-24	3.5	CVE-2021-32624 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	having `read` access control configured. If you use private fields or lists, you may be impacted. No patches exist at this time. There are no workarounds at this time			
lifterlms -- lifterlms	The 'State' field of the Edit profile page of the LMS by LifterLMS – Online Course, Membership & Learning Management System Plugin for WordPress plugin before 4.21.1 is not properly sanitised when output in the About section of the profile page, leading to a stored Cross-Site Scripting issue. This could allow low privilege users (such as students) to elevate their privilege via an XSS attack when an admin will view their profile.	2021-05-24	3.5	CVE-2021-24308 MISC CONFIRM MISC
neox -- hana_flv_player	The Hana Flv Player WordPress plugin through 3.1.3 is vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) vulnerability within the 'Default Skin' field.	2021-05-24	3.5	CVE-2021-24302 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpmywind -- phpmywind	Cross Site Scripting (XSS) in PHPMyWind v5.5 allows remote attackers to execute arbitrary code by injecting scripts into the parameter "$cfg_switchshow" of component " /admin/web_config.php".	2021-05-27	3.5	CVE-2020-18230 MISC
phpmywind -- phpmywind	Cross Site Scripting (XSS) in PHPMyWind v5.5 allows remote attackers to execute arbitrary code by injecting scripts into the parameter "$cfg_copyright" of component " /admin/web_config.php".	2021-05-27	3.5	CVE-2020-18229 MISC
plone -- plone	Plone through 5.2.4 allows stored XSS attacks (by a Contributor) by uploading an SVG or HTML document.	2021-05-21	3.5	CVE-2021-33512 MISC MLIST
plone -- plone	Plone through 5.2.4 allows XSS via the inline_diff methods in Products.CMFDiffTool.	2021-05-21	3.5	CVE-2021-33513 MISC MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
plone -- plone	Plone through 5.2.4 allows XSS via a full name that is mishandled during rendering of the ownership tab of a content item.	2021-05-21	3.5	CVE-2021-33508 MISC MLIST
postbird_project -- postbird	Postbird 0.8.4 allows stored XSS via the onerror attribute of an IMG element in any PostgreSQL database table. This can result in reading local files via vectors involving XMLHttpRequest and open of a file:/// URL, or discovering PostgreSQL passwords via vectors involving Window.localStorage and savedConnections.	2021-05-25	3.5	CVE-2021-33570 MISC MISC MISC MISC MISC
shopizer -- shopizer	A stored cross-site scripting (XSS) vulnerability in Shopizer before 2.17.0 allows remote attackers to inject arbitrary web script or HTML via customer_name in various forms of store administration. It is saved in the database. The code is executed for any user of store administration when information is fetched from the backend, e.g., in admin/customers/list.html.	2021-05-24	3.5	CVE-2021-33561 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
shopizer -- shopizer	A reflected cross-site scripting (XSS) vulnerability in Shopizer before 2.17.0 allows remote attackers to inject arbitrary web script or HTML via the ref parameter to a page about an arbitrary product, e.g., a product/insert-product-name-here.html/ref= URL.	2021-05-24	3.5	CVE-2021-33562 MISC MISC MISC
zephyrproject -- zephyr	Incorrect Error Handling in Bluetooth HCI core. Zephyr versions >= v1.14.2, >= v2.2.0 contain NULL Pointer Dereference (CWE-476). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-gc66-xfrc-24qr	2021-05-25	3.3	CVE-2020-10066 MISC
zephyrproject -- zephyr	Zephyr Bluetooth unchecked packet data results in denial of service. Zephyr versions >= v1.14.2, >= v2.2.0 contain Improper Handling of Parameters (CWE-233). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-f6vh-7v4x-8fjp	2021-05-25	3.3	CVE-2020-10069 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zephyrproject -- zephyr	Remote Denial of Service in LwM2M do_write_op_tlv. Zephyr versions >= 1.14.2, >= 2.2.0 contain Improper Input Validation (CWE-20), Loop with Unreachable Exit Condition ('Infinite Loop') (CWE-835). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-g9mg-fj58-6fqh	2021-05-25	2.1	CVE-2020-13602 MISC