Vulnerability Summary for the Week of May 3, 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
ambarella -- oryx_rtsp_server	A buffer overflow in the RTSP service of the Ambarella Oryx RTSP Server 2020-01-07 allows an unauthenticated attacker to send a crafted RTSP request, with a long digest authentication header, to execute arbitrary code in parse_authentication_header() in libamprotocol-rtsp.so.1 in rtsp_svc (or cause a crash). This allows remote takeover of a Furbo Dog Camera, for example.	2021-04-30	10	CVE-2020-24918 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ampache -- ampache	Ampache before version 4.2.2 allows unauthenticated users to perform SQL injection. Refer to the referenced GitHub Security Advisory for details and a workaround. This is fixed in version 4.2.2 and the development branch.	2021-04-30	7.5	CVE-2020-15153 MISC MISC CONFIRM
cisco -- anyconnect_secure_mobility_client	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory.	2021-05-06	7.2	CVE-2021-1496 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- anyconnect_secure_mobility_client	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory.	2021-05-06	7.2	CVE-2021-1430 CISCO
cisco -- anyconnect_secure_mobility_client	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application.	2021-05-06	7.2	CVE-2021-1429 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory.			
cisco -- anyconnect_secure_mobility_client	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these	2021-05-06	7.2	CVE-2021-1428 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerabilities, see the Details section of this advisory.			
cisco -- anyconnect_secure_mobility_client	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory.	2021-05-06	7.2	CVE-2021-1427 CISCO
cisco -- anyconnect_secure_mobility_client	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an	2021-05-06	7.2	CVE-2021-1426 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory.			
dell -- hybrid_client	Dell Hybrid Client versions prior to 1.5 contain a missing authentication for a critical function vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to gain root level access to the system.	2021-04-30	7.2	CVE-2021-21535 MISC
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to insecure inter-deployment communication. An attacker that is able to	2021-05-05	7.5	CVE-2020-4979 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	comprimise or spoof traffic between hosts may be able to execute arbitrary commands. IBM X-Force D: 192538.			
klibc_project -- klibc	An issue was discovered in klibc before 2.0.9. Multiple possible integer overflows in the cpio command on 32-bit systems may result in a buffer overflow or other security impact.	2021-04-30	7.5	CVE-2021-31872 MISC MISC MISC MLIST
klibc_project -- klibc	An issue was discovered in klibc before 2.0.9. Multiplication in the calloc() function may result in an integer overflow and a subsequent heap buffer overflow.	2021-04-30	7.5	CVE-2021-31870 MISC MISC MISC MLIST
projectworlds -- online_book_store_project_in_php	SQL Injection vulnerability in Online Book Store v1.0 via the publisher parameter to edit_book.php, which could let a	2021-05-06	7.5	CVE-2020-19114 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote malicious user execute arbitrary code.			
projectworlds -- online_book_store_project_in_php	SQL Injection vulnerability in Online Book Store v1.0 via the bookisbn parameter to admin_delete.php, which could let a remote malicious user execute arbitrary code.	2021-05-06	7.5	CVE-2020-19112 MISC
projectworlds -- online_book_store_project_in_php	SQL Injection vulnerability in Online Book Store v1.0 via the bookisbn parameter to book.php parameter, which could let a remote malicious user execute arbitrary code.	2021-05-06	7.5	CVE-2020-19110 MISC
projectworlds -- online_book_store_project_in_php	SQL Injection vulnerability in Online Book Store v1.0 via the bookisbn parameter to admin_edit.php, which could let a remote malicious user execute arbitrary code.	2021-05-06	7.5	CVE-2020-19109 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
projectworlds -- online_book_store_project_in_php	SQL Injection vulnerability in Online Book Store v1.0 via the pubid parameter to bookPerPub.php, which could let a remote malicious user execute arbitrary code.	2021-05-06	7.5	CVE-2020-19108 MISC
projectworlds -- online_book_store_project_in_php	SQL Injection vulnerability in Online Book Store v1.0 via the isbn parameter to edit_book.php, which could let a remote malicious user execute arbitrary code.	2021-05-06	7.5	CVE-2020-19107 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
chamilo -- chamilo_lms	Chamilo LMS 1.11.10 is affected by Cross Site Request Forgery (CSRF) via the edit_user function by targeting an admin user.	2021-05-06	6.8	CVE-2020-23127 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
codesys -- development_system	CODESYS Development System 3 before 3.5.17.0 displays or executes malicious documents or files embedded in libraries without first checking their validity.	2021-05-03	4.6	CVE-2021-29239 MISC MISC MISC
dell -- debutil_2_3.sys	Dell dbutil_2_3.sys driver contains an insufficient access control vulnerability which may lead to escalation of privileges, denial of service, or information disclosure. Local authenticated user access is required.	2021-05-04	4.6	CVE-2021-21551 MISC
drupal -- drupal	Cross-site scripting vulnerability in Drupal Core. Drupal AJAX API does not disable JSONP by default, allowing for an XSS attack. This issue affects: Drupal Drupal Core 7.x versions prior to 7.73; 8.8.x versions prior to 8.8.10; 8.9.x	2021-05-05	4.3	CVE-2020-13666 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions prior to 8.9.6; 9.0.x versions prior to 9.0.6.			
google -- chrome	Insufficient data validation in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21231 MISC MISC GENTOO DEBIAN
google -- chrome	Insufficient data validation in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21227 MISC MISC GENTOO DEBIAN
google -- chrome	Incorrect security UI in downloads in Google Chrome on Android prior to 90.0.4430.93 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2021-04-30	4.3	CVE-2021-21229 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				GENTOO DEBIAN
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 90.0.4430.93 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	2021-04-30	4.3	CVE-2021-21228 MISC MISC GENTOO DEBIAN
google -- chrome	Use after free in Dev Tools in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21232 MISC MISC GENTOO DEBIAN
google -- chrome	Type confusion in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21230 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				GENTOO DEBIAN
google -- chrome	Heap buffer overflow in ANGLE in Google Chrome on Windows prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21233 MISC MISC GENTOO DEBIAN
google -- cloud_iot_device_sdk_for_embedded_c	In IoT Devices SDK, there is an implementation of calloc() that doesn't have a length check. An attacker could pass in memory objects larger than the buffer and wrap around to have a smaller buffer than required, allowing the attacker access to the other parts of the heap. We recommend upgrading the Google Cloud IoT Device SDK for Embedded C used to 1.0.3 or greater.	2021-05-04	4.6	CVE-2021-22547 CONFIRM CONFIRM
gosaml2_project -- gosaml2	This affects all versions of package github.com/russellhaering/gosaml2.	2021-04-30	5	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	There is a crash on nil-pointer dereference caused by sending malformed XML signatures.			7731 CONFIRM CONFIRM
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 and 7.4 when decompressing or verifying signature of zip files processes data in a way that may be vulnerable to path traversal attacks. IBM X-Force ID: 192905.	2021-05-05	4	CVE-2020-4993 CONFIRM XF
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 and 7.4 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: 191748.	2021-05-05	4.6	CVE-2020-4932 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 and 7.4 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: 196017.	2021-05-05	4.3	CVE-2021-20397 XF CONFIRM
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 and 7.4 may vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 193245.	2021-05-05	5.5	CVE-2020-5013 CONFIRM XF
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 and 7.4 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	2021-05-05	4.6	CVE-2021-20401 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	internal data. IBM X-Force ID: 196075.			
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 and 7.4 could disclose sensitive information about other domains which could be used in further attacks against the system. IBM X-Force ID: 190907.	2021-05-05	4	CVE-2020-4883 XF CONFIRM
idreamsoft -- icms	Path Traversal in iCMS v7.0.13 allows remote attackers to delete folders by injecting commands into a crafted HTTP request to the "do_del()" method of the component "database.admincp.php".	2021-04-30	6.4	CVE-2020-18070 MISC
klibc_project -- klibc	An issue was discovered in klibc before 2.0.9. An integer overflow in the cpio command may result in a NULL pointer dereference on 64-bit systems.	2021-04-30	5	CVE-2021-31871 MISC MISC MISC MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mongodb -- mongodb	A user authorized to performing a specific type of find query may trigger a denial of service. This issue affects: MongoDB Inc. MongoDB Server v4.4 versions prior to 4.4.4.	2021-04-30	4	CVE-2021-20326 CONFIRM
open-xchange -- open-xchange_appsuite	OX App Suite 7.10.4 and earlier allows XSS via a crafted contact object (payload in the position or company field) that is mishandled in the App Suite UI on a smartphone.	2021-04-30	4.3	CVE-2021-31934 MISC
open-xchange -- open-xchange_appsuite	OX App Suite 7.10.4 and earlier allows XSS via a crafted distribution list (payload in the common name) that is mishandled in the scheduling view.	2021-04-30	4.3	CVE-2021-31935 MISC
open-xchange -- open-xchange_appsuite	OX App Suite 7.10.4 and earlier allows SSRF via a snippet.	2021-04-30	4	CVE-2020-28943 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
open-xchange -- open-xchange_appsuite	OX App Suite 7.10.4 and earlier allows XSS via crafted content to reach an undocumented feature, such as ![](http://onerror=Function.constructor, in a Notes item.	2021-05-03	4.3	CVE-2020-28945 MISC MISC
open-xchange -- ox_guard	OX Guard 2.10.4 and earlier allows a Denial of Service via a WKS server that responds slowly or with a large amount of data.	2021-04-30	5	CVE-2020-28944 MISC MISC
rkyv_project -- rkyv	An issue was discovered in the rkyv crate before 0.6.0 for Rust. When an archive is created via serialization, the archive content may contain uninitialized values of certain parts of a struct.	2021-04-30	5	CVE-2021-31919 MISC
yzmcms -- yzmcms	Cross Site Scripting (XSS) in yzmCMS v5.2 allows remote attackers to execute arbitrary code by injecting commands into the "referer" field of a POST request to	2021-04-30	4.3	CVE-2020-18084 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the component "/member/index/login.html" when logging in.			

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- anyconnect_secure_mobility_client	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client Software could allow an authenticated, local attacker to overwrite VPN profiles on an affected device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process. A successful exploit	2021-05-06	2.1	CVE-2021-1519 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could allow the attacker to modify VPN profile files. To exploit this vulnerability, the attacker must have valid credentials on the affected system.			
crocoblock -- jetwidgets_for_elementor	The “JetWidgets For Elementor” WordPress Plugin before 1.0.9 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method.	2021-05-05	3.5	CVE-2021-24268 CONFIRM MISC
dell -- hybrid_client	Dell Hybrid Client versions prior to 1.5 contain an information exposure vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to gain access to sensitive information via the local API.	2021-04-30	2.1	CVE-2021-21534 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- hybrid_client	Dell Hybrid Client versions prior to 1.5 contain an information exposure vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to register the client to a server in order to view sensitive information.	2021-04-30	2.1	CVE-2021-21536 MISC
dell -- hybrid_client	Dell Hybrid Client versions prior to 1.5 contain an information exposure vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to view and exfiltrate sensitive information on the system.	2021-04-30	2.1	CVE-2021-21537 MISC
ibm -- flashsystem_900_firmware	IBM FlashSystem 900 1.5.2.9 and 1.6.1.3 user management GUI is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality	2021-05-04	3.5	CVE-2020-4987 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 192702.			
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 and 7.4 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: 191706.	2021-05-05	3.5	CVE-2020-4929 CONFIRM XF
salesagility -- suitecrm	XSS in the client account page in SuiteCRM before 7.11.19 allows an attacker to inject JavaScript via the name field	2021-04-30	3.5	CVE-2021-31792 MISC MISC MISC