Vulnerability Summary for the Week of May 31, 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
gnome -- gdk-pixbuf	A flaw was found in gdk-pixbuf in versions before 2.42.0. An integer wraparound leading to an out of bounds write can occur when a crafted GIF image is loaded. An attacker may cause applications to crash or could potentially execute code on the victim system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-28	8.3	CVE-2021-20240 MISC FEDORA FEDORA FEDORA
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 DQM API allows submitting of all control requests in unauthenticated sessions. This allows a remote attacker who can access a valid CA	2021-06-01	7.5	CVE-2020-4561

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	endpoint to read and write files to the Cognos Analytics system. IBM X-Force ID: 183903.			CONFIRM XF
linux -- linux_kernel	There is a flaw reported in the Linux kernel in versions before 5.9 in drivers/gpu/drm/nouveau/nouveau_sgdma.c in nouveau_sgdma_create_ttm in Nouveau DRM subsystem. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker with a local account with a root privilege, can leverage this vulnerability to escalate privileges and execute code in the context of the kernel.	2021-05-28	7.2	CVE-2021-20292 MISC
linuxfoundation -- dex	A vulnerability exists in the SAML connector of the github.com/dexidp/dex library used to process SAML Signature Validation. This flaw allows an attacker to bypass SAML authentication. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. This flaw affects dex versions before 2.27.0.	2021-05-28	7.5	CVE-2020-27847 MISC MISC MISC
zeromq -- zeromq	A flaw was found in the ZeroMQ server in versions before 4.3.3. This flaw allows a malicious client to cause a stack buffer overflow on the server by sending crafted topic subscription requests and then unsubscribing. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-05-28	7.5	CVE-2021-20236 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cesanta -- mjs	Stack overflow vulnerability in parse_plus_minus Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36372 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_statement Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36368 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_value Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36366 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_comparison Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36374 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cesanta -- mjs	Stack overflow vulnerability in parse_array Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-18392 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_equality Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36375 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_shifts Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36373 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_statement_list Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36369 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_mul_div_rem Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36371 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cesanta -- mjs	Stack overflow vulnerability in parse_unary Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36370 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_block Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36367 MISC
css-what_project -- css-what	The css-what package before 5.0.1 for Node.js does not ensure that attribute parsing has Linear Time Complexity relative to the size of the input.	2021-05-28	5	CVE-2021-33587 MISC
gnu -- gama	A NULL-pointer deference issue was discovered in GNU_gama::set() in ellipsoid.h in Gama 2.04 which can lead to a denial of service (DOS) via segment faults caused by crafted inputs.	2021-05-28	5	CVE-2020-18395 MISC
ibm -- application_gateway	IBM Security Verify Access 20.07 could allow a remote attacker to send a specially crafted HTTP GET request that could cause the application to crash.	2021-06-01	5	CVE-2021-20576 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain credentials from a user's browser via incorrect autocomplete settings in New Content Backup page. IBM X-Force ID: 172130.	2021-06-01	5	CVE-2019-4724 XF CONFIRM
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain credentials from a user's browser via incorrect autocomplete settings in New Data Server Connection page. IBM X-Force ID: 172129.	2021-06-01	5	CVE-2019-4723 CONFIRM XF
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain sensitive information, caused by the failure to set the secure flag for a sensitive cookie in an HTTPS session. A remote attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 163780.	2021-06-01	4	CVE-2019-4471 CONFIRM XF
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to an 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: 172533.	2021-06-01	5.5	CVE-2019-4730 CONFIRM XF
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to inject malicious HTML code that when viewed	2021-06-01	6.8	CVE-2020-4520

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	by the authenticated victim would execute the code. IBM X-Force ID: 182395.			XF CONFIRM
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to an 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: 176607.	2021-06-01	6.4	CVE-2020-4300 CONFIRM XF
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain sensitive information via a stack trace due to mishandling of certain error conditions. IBM X-Force ID: 172128.	2021-06-01	4	CVE-2019-4722 CONFIRM XF
ibm -- security_verify_access	IBM Security Verify Access 20.07 could disclose sensitive information in HTTP server headers that could be used in further attacks against the system. IBM X-Force ID: 199398.	2021-06-01	5	CVE-2021-20585 XF CONFIRM
idreamsoft -- icms	A Cross Site Request Forgery (CSRF) vulnerability was discovered in iCMS 7.0.16 which can allow an attacker to execute arbitrary web scripts.	2021-05-28	6.8	CVE-2020-26641 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kiali -- kiali	An authentication bypass vulnerability was found in Kiali in versions before 1.31.0 when the authentication strategy `OpenID` is used. When RBAC is enabled, Kiali assumes that some of the token validation is handled by the underlying cluster. When OpenID `implicit flow` is used with RBAC turned off, this token validation doesn't occur, and this allows a malicious user to bypass the authentication.	2021-05-28	5.8	CVE-2021-20278 MISC MISC
naver -- comic_viewer	An exposed remote debugging port in Naver Comic Viewer prior to 1.0.15.0 allowed a remote attacker to execute arbitrary code via a crafted HTML page.	2021-05-28	6.8	CVE-2021-33591 CONFIRM
openldap -- openldap	A flaw was found in OpenLDAP in versions before 2.4.56. This flaw allows an attacker who sends a malicious packet processed by OpenLDAP to force a failed assertion in csnNormalize23(). The highest threat from this vulnerability is to system availability.	2021-05-28	5	CVE-2020-25710 MLIST MISC DEBIAN MISC
redhat -- 389_directory_server	When using a sync_repl client in 389-ds-base, an authenticated attacker can cause a NULL pointer dereference using a specially crafted query, causing a crash.	2021-05-28	4	CVE-2021-3514 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
redhat -- keycloak	A flaw was found in keycloak in versions before 13.0.0. A Self Stored XSS attack vector escalating to a complete account takeover is possible due to user-supplied data fields not being properly encoded and Javascript code being used to process the data. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-28	6.8	CVE-2021-20195 MISC
redhat -- keycloak	A flaw was found in Keycloak before version 12.0.0 where it is possible to update the user's metadata attributes using Account REST API. This flaw allows an attacker to change its own NameID attribute to impersonate the admin user for any particular application.	2021-05-28	4.9	CVE-2020-27826 MISC
seacms -- seacms	A cross-site scripting (XSS) vulnerability has been discovered in the login page of SeaCMS version 11 which allows an attacker to inject arbitrary web script or HTML.	2021-05-28	4.3	CVE-2020-26642 MISC
spice_project -- spice	A flaw was found in spice in versions before 0.14.92. A DoS tool might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection.	2021-05-28	5	CVE-2021-20201 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trim-newlines_project -- trim-newlines	The trim-newlines package before 3.0.1 and 4.x before 4.0.1 for Node.js has an issue related to regular expression denial-of-service (ReDoS) for the .end() method.	2021-05-28	5	CVE-2021-33623 MISC CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 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: 170964.	2021-06-01	3.5	CVE-2019-4653 XF CONFIRM
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 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: 178506.	2021-06-01	3.5	CVE-2020-4354 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	A flaw was found in the Linux kernel in versions before 5.4.92 in the BPF protocol. This flaw allows an attacker with a local account to leak information about kernel internal addresses. The highest threat from this vulnerability is to confidentiality.	2021-05-28	2.1	CVE-2021-20239 MISC
qemu -- qemu	A NULL pointer dereference flaw was found in the SCSI emulation support of QEMU in versions before 6.0.0. This flaw allows a privileged guest user to crash the QEMU process on the host, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	2021-05-28	2.1	CVE-2020-35504 MLIST MISC MISC