Known Exploited Vulnerabilities Catalog

Download CSV version </sites/default/files/csv/known_exploited_vulnerabilities.csv>

Download JSON version </sites/default/files/feeds/known_exploited_vulnerabilities.json>

Download JSON schema </sites/default/files/feeds/known_exploited_vulnerabilities_schema.json>

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities </known_exploited_vulnerabilities>

Show 10 entries Search:

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2023-25717 <https://nvd.nist.gov/vuln/detail/cve-2023-25717>	Ruckus Wireless	Multiple Products	Multiple Ruckus Wireless Products CSRF and RCE Vulnerability	2023-05-12	Ruckus Wireless Access Point (AP) software contains an unspecified vulnerability in the web services component. If the web services component is enabled on the AP, an attacker can perform cross-site request forgery (CSRF) or remote code execution (RCE). This vulnerability impacts Ruckus ZoneDirector, SmartZone, and Solo APs.	Apply updates per vendor instructions or disconnect product if it is end-of-life.	2023-06-02	https://support.ruckuswireless.com/security_bulletins/315
CVE-2021-3560 <https://nvd.nist.gov/vuln/detail/cve-2021-3560>	Red Hat	Polkit	Red Hat Polkit Incorrect Authorization Vulnerability	2023-05-12	Red Hat Polkit contains an incorrect authorization vulnerability through the bypassing of credential checks for D-Bus requests, allowing for privilege escalation.	Apply updates per vendor instructions.	2023-06-02	https://bugzilla.redhat.com/show_bug.cgi?id=1961710
CVE-2014-0196 <https://nvd.nist.gov/vuln/detail/cve-2014-0196>	Linux	Kernel	Linux Kernel Race Condition Vulnerability	2023-05-12	Linux Kernel contains a race condition vulnerability within the n_tty_write function that allows local users to cause a denial-of-service or gain privileges via read and write operations with long strings.	The impacted product is end-of-life and should be disconnected if still in use.	2023-06-02	https://lkml.iu.edu/hypermail/linux/kernel/1609.1/02103.html
CVE-2010-3904 <https://nvd.nist.gov/vuln/detail/cve-2010-3904>	Linux	Kernel	Linux Kernel Improper Input Validation Vulnerability	2023-05-12	Linux Kernel contains an improper input validation vulnerability in the Reliable Datagram Sockets (RDS) protocol implementation that allows local users to gain privileges via crafted use of the sendmsg and recvmsg system calls.	The impacted product is end-of-life and should be disconnected if still in use.	2023-06-02	https://lkml.iu.edu/hypermail/linux/kernel/1601.3/06474.html
CVE-2015-5317 <https://nvd.nist.gov/vuln/detail/cve-2015-5317>	Jenkins	Jenkins User Interface (UI)	Jenkins User Interface (UI) Information Disclosure Vulnerability	2023-05-12	Jenkins User Interface (UI) contains an information disclosure vulnerability that allows users to see the names of jobs and builds otherwise inaccessible to them on the "Fingerprints" pages.	Apply updates per vendor instructions.	2023-06-02	https://www.jenkins.io/security/advisory/2015-11-11/

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2016-3427 <https://nvd.nist.gov/vuln/detail/cve-2016-3427>	Oracle	Java SE and JRockit	Oracle Java SE and JRockit Unspecified Vulnerability	2023-05-12	Oracle Java SE and JRockit contains an unspecified vulnerability that allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Java Management Extensions (JMX). This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.	Apply updates per vendor instructions.	2023-06-02	https://www.oracle.com/security-alerts/cpuapr2016v3.html
CVE-2016-8735 <https://nvd.nist.gov/vuln/detail/cve-2016-8735>	Apache	Tomcat	Apache Tomcat Remote Code Execution Vulnerability	2023-05-12	Apache Tomcat contains an unspecified vulnerability that allows for remote code execution if JmxRemoteLifecycleListener is used and an attacker can reach Java Management Extension (JMX) ports. This CVE exists because this listener wasn't updated for consistency with the Oracle patched issues for CVE-2016-3427 which affected credential types.	Apply updates per vendor instructions.	2023-06-02	https://tomcat.apache.org/security-9.html
CVE-2023-29336 <https://nvd.nist.gov/vuln/detail/cve-2023-29336>	Microsoft	Win32k	Microsoft Win32K Privilege Escalation Vulnerability	2023-05-09	Microsoft Win32k contains an unspecified vulnerability that allows for privilege escalation up to SYSTEM privileges.	Apply updates per vendor instructions.	2023-05-30	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29336
CVE-2023-1389 <https://nvd.nist.gov/vuln/detail/cve-2023-1389>	TP-Link	Archer AX21	TP-Link Archer AX-21 Command Injection Vulnerability	2023-05-01	TP-Link Archer AX-21 contains a command injection vulnerability that allows for remote code execution.	Apply updates per vendor instructions.	2023-05-22	https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware
CVE-2021-45046 <https://nvd.nist.gov/vuln/detail/cve-2021-45046>	Apache	Log4j2	Apache Log4j2 Deserialization of Untrusted Data Vulnerability	2023-05-01	Apache Log4j2 contains a deserialization of untrusted data vulnerability due to the incomplete fix of CVE-2021-44228, where the Thread Context Lookup Pattern is vulnerable to remote code execution in certain non-default configurations.	Apply updates per vendor instructions.	2023-05-22	https://logging.apache.org/log4j/2.x/security.html

Showing 1 to 10 of 933 entries Previous 1 2 3 4 5 … 94 Next

Back to top

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools> **News & Events** </news-events> **Careers** </careers> **About** </about>

CISA Central

888-282-0870 Central@cisa.dhs.gov