Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly December 2023

This report primarily analyzes the top vulnerabilities disclosed across 8 major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from December 1 to 31, 2023. It includes the total number of vulnerabilities disclosed within the reporting period, the number of critical and zero-day vulnerabilities disclosed, the number of vulnerabilities actively exploited at the time of writing, and additional major trends and noteworthy vulnerabilities.

Key Findings

- In December 2023, 6 zero-day vulnerabilities were identified in products from Future X Communication, Google Chrome, QNAP, Unitronic, Apache Struts 2, and Android.
- Google issued an update to address a high-severity zero-day vulnerability, CVE-2023-7024, in Chrome, which makes it the eighth Chrome zero-day vulnerability disclosed since the beginning of 2023.
- 12 of the approximately 2,500 vulnerabilities disclosed in December 2023 were high-risk, according to Recorded Future data.
- Atlassian disclosed 4 critical remote code execution vulnerabilities.
- Microsoft disclosed no high-risk zero-day vulnerabilities for the first time in 2023.

CVE Monthly Prominent Vulnerability Disclosures

In December 2023, we identified 12 high-risk vulnerabilities, 6 of which were zero-day vulnerabilities known to be exploited in the wild.

This month's principal vulnerability trend was the continuation of attacks exploiting vulnerabilities in enterprise software to deploy ransomware, which can lead to operational disruption and data compromise. In December 2023, threat actors exploited vulnerabilities that were disclosed and patched in previous months in Atlassian Confluence (CVE-2023-22515, CVE-2023-22518), Citrix Netscaler ADC and Gateway (CVE-2023-4966, “Citrix Bleed”), and Oracle WebLogic Server (CVE-2020-14883) to deploy ransomware. For example, security researchers continued to observe ongoing mass exploitation of “Citrix Bleed”, or CVE-2023-4966, a zero-day vulnerability affecting Citrix NetScaler ADC and NetScaler Gateway devices. Threat actors target systems like Atlassian Confluence, Citrix NetScaler ADC and Gateway, and Oracle WebLogic Server because they enable access to sensitive data and are widely used in critical business operations. These attacks can potentially cause significant organizational disruption, which in turn may increase the chances of cybercriminal groups getting a payout.

Continuing a trend that began in September 2023, Atlassian disclosed and patched 4 additional critical vulnerabilities in December 2023. While Atlassian did not mention whether the vulnerabilities are being actively exploited, these vulnerabilities pose significant remote execution risks, including template injection in Confluence and privileged execution through Assets Discovery. Users are advised to quickly update their software to the patched versions to prevent potential exploits. As described in our October 2023 CVE Monthly report, a state-sponsored group, Storm-0062, exploited a separate Confluence vulnerability (CVE-2023-22515). While the exploitation methods for these vulnerabilities differ, the potential impacts — if the vulnerabilities are successfully exploited — can allow threat actors to gain privileged access within Confluence Data Center and Confluence Servers environments. Organizations should conduct vulnerability assessments for Confluence Data Center and Confluence Servers and ensure that vulnerable instances are patched immediately.

Recorded Future also observed the disclosure of CVE-2023-32725. The exploit occurs when an administrator adds an attacker-crafted URL to a Zabbix widget, likely through social engineering. Once added, the threat actor can capture the administrator's session cookie. This session cookie enables the threat actor to access the Zabbix instance with administrative privileges, posing a

significant security risk. Although security researchers have not observed active exploitation in the wild of this vulnerability, and although it is not classified as high risk at the time of writing, administrators should patch the vulnerability in a timely manner due to the security risk it poses.

Below, we further discuss the top vulnerabilities disclosed in December 2023:

Atlassian Patched 4 Critical Vulnerabilities Allowing Remote Code Execution
Atlassian issued a series of critical security updates on December 6, 2023, addressing 4 severe vulnerabilities in its product that could lead to remote code execution. The vulnerabilities include a deserialization issue in the snakeyaml library (CVE-2022-1471), a remote code execution flaw in Confluence Server and Data Center (CVE-2023-22522), a similar vulnerability in Assets Discovery for Jira Service Management Cloud, Server, and Data Center (CVE-2023-22523), and a vulnerability in the Atlassian Companion app for macOS (CVE-2023-22524).

Google Patches Eighth Chrome Zero-Day Vulnerability of 2023
On December 20, 2023, Google issued an update to address a high-severity zero-day vulnerability, CVE-2023-7024, in Chrome, the eighth Chrome zero-day vulnerability disclosed since the beginning of 2023. CVE-2023-7024 is a heap buffer overflow vulnerability in WebRTC in Google Chrome versions prior to 120.0.6099.129. Exploitation of CVE-2023-7024 can enable a remote attacker to exploit heap corruption via a crafted HTML page. Clément Lecigne and Vlad Stolyarov, members of Google's Threat Analysis Group (TAG), discovered and reported the vulnerability on December 19, 2023, and a patch was issued the following day.

At this time, there is no additional information in open sources about how CVE-2023-7024 was exploited in the wild, nor what damage it can cause. Google noted in its advisory that access to the precise details of this vulnerability would be restricted until Google verifies that most Chrome users have implemented the updates necessary to remediate CVE-2023-7024. Google also noted that it would restrict access to information about CVE-2023-7024 if the vulnerability were found to affect other vendor implementations of WebRTC, likely to give other vendors a chance to address the vulnerability prior to disclosure.

Critical Vulnerability in Apache Struts 2 Allows for Remote Code Execution
A critical vulnerability in Apache Struts 2, a popular framework for enterprise web applications, has been identified as CVE-2023-50164. The vulnerability stems from improper handling of file upload parameters, according to Cisco's security advisory on December 12, 2023. Initially reported by researcher Steven Seeley, this security flaw allows for unauthorized path traversal, allowing threat actors to manipulate file upload parameters and upload and execute malicious files. This vulnerability also has the potential for remote code execution and does not require authentication for exploitation.

Apache has released patches in versions 2.5.33 and 6.3.0.2 of the Struts framework, and there are no known workarounds. At the time of writing, this vulnerability is not known to be exploited in the wild.

Organizations using older versions of Apache Struts 2, particularly any version prior to 2.5.33 or 6.3.0.2, are vulnerable to this security flaw, and developers must apply the aforementioned patches immediately. Maintaining updated software and a robust vulnerability management process are essential to safeguard against vulnerability-based threats.

CISA Released an Alert Urging Manufacturers to Eliminate Default Passwords on Internet-Exposed Systems After Recent ICS Attacks

CISA issued an alert on December 15, 2023, urging manufacturers to avoid using default passwords for systems exposed to the internet. This alert was issued 2 weeks after a threat actor associated with the Iranian government took control of Industrial Control Systems at the Municipal Water Authority of Aliquippa in Pennsylvania and multiple other water utilities across the US. The attacker exploited a Unitronics Vision series programmable logic controller (PLC) that had a weak default password exposed on the internet. CISA assigned CVE-2023-6448 to this Unitronic product vulnerability, in which default administrative passwords were used, with a CVSS score of 9.8.

CVE Monthly Prominent Vulnerability Disclosures

In the table below, actively exploited vulnerabilities affecting the 8 major software vendors are highlighted in gray.

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/ Component	Zero-Day
1	**CVE-2023-49897**	99	Future X Communications (FXC) outlet routers	A security flaw related to operating system (OS) command injection that is present in both AE1021PE and AE1021 firmware, versions 2.0.9 and earlier. This vulnerability allows an attacker with login access to the product to execute any OS command.	Yes
2	**CVE-2023-7024**	99	Google Chrome	A heap buffer overflow vulnerability in WebRTC in Google Chrome versions prior to 120.0.6099.129. Exploitation of CVE-2023-7024 can enable a remote threat actor to exploit heap corruption via a crafted HTML page.	Yes
3	**CVE-2023-47565**	99	QNAP VioStor Network Video Recorder (NVR) Devices	Legacy QNAP VioStor NVR models operating on QVR Firmware 4.x are susceptible to an OS command injection vulnerability. If exploited, threat actors authenticated in the network can conduct remote code execution.	Yes
4	**CVE-2023-6448**	96	Unitronic VisiLogic	Prior to version 9.9.00, Unitronics VisiLogic, used in Vision and Samba PLCs and human-machine interfaces (HMIs), is configured with a default administrative password. This configuration makes systems vulnerable to unauthorized administrative control by threat actors who gain network access.	Yes
5	**CVE-2023-49954**	95	3CX CRM Integration	A critical structured query language (SQL) injection vulnerability in 3CX CRM integration that threat actors can exploit to compromise significant amounts of data.	No
6	**CVE-2023-50164**	89	Apache Struts 2	A path traversal vulnerability, allowing threat actors to manipulate file upload parameters and upload and execute malicious files. This vulnerability also has the potential for remote code execution and does not require authentication for	Yes

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/ Component	Zero-Day
				exploitation.	
7	**CVE-2023-51385**	79	OpenSSH ProxyCommand	OS command injection vulnerability that can allow threat actors to perform shell injection on vulnerable servers.	No
8	**CVE-2023-22522**	79	Atlassian Confluence Data Center and Confluence Server	Critical remote code execution vulnerability that can allow threat actors to inject "unsafe user input" into Confluence pages.	No
9	**CVE-2023-22524**	79	Atlassian Companion App for MacOS	Critical remote code execution vulnerability affecting the Companion App for MacOS.	No
10	**CVE-2023-40088**	79	Android System Component	Critical security vulnerability in the Android system component that threat actors can exploit for remote code execution.	Yes
11	**CVE-2023-6553**	79	WordPress Backup Migration plugin	The unauthenticated remote code execution vulnerability can enable threat actors to take control of targeted websites by executing remote code through injecting malicious Hypertext Processor (PHP) code, facilitated via the plugin's "`/includes/backup-heart.php`" file.	No
12	**CVE-2023-22523**	75	Atlassian Assets Discovery Cloud	Critical remote code execution vulnerability affecting the Assets Discovery for Jira Service Management Cloud, Server, and Data Center.	No

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence. Learn more at recordedfuture.com.