Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly May 2024

Executive Summary

In May 2024, we did not identify any instances of massive zero-day exploitation. We identified 258 high-risk vulnerabilities, seven of which were actively exploited in the wild to execute code remotely, corrupt data, crash targeted systems, escalate privileges, and perform unauthorized memory access.

This month, Google disclosed and patched four zero-day vulnerabilities (CVE-2024-4947, CVE-2024-5274, CVE-2024-4671, and CVE-2024-4761). Unnamed threat actors actively exploited these vulnerabilities and, in some instances, publicly released proof-of-concept (PoC) exploits. Since the beginning of 2024, Google has patched eight Chrome zero-days. Additionally, among 61 security vulnerabilities in its May 2024 Patch Tuesday update, Microsoft patched two vulnerabilities (CVE-2024-30040 and CVE-2024-30051) that were actively exploited by unknown threat actors. CVE-2024-30051 was exploited in cyberattacks to deploy Qakbot. We have not identified evidence of these vulnerabilities being actively exploited following Google's and Microsoft's patch releases.

Many instances in which services were affected by these vulnerabilities, aside from instances involving CVE-2024-4947, are publicly discoverable via internet scan. Combined with the ease of exploiting these vulnerabilities, their confirmed, active exploitation, and the availability of PoC exploit code make the vulnerabilities critical to prioritize for immediate patching.

Key Findings

- We identified seven high-risk vulnerabilities that were exploited in the wild this month; they were found in software by vendors like Justice AV Solutions (JAVS), Google, and Microsoft.
- Although we did not see them being actively exploited, we identified two vulnerabilities in BIG-IP Next Central Manager 20.0.1 and 20.1.0 and version 5.2 of Confluence Data Center and Server associated with a public PoC exploit code, enabling threat actors to exploit them more easily.
- A vulnerability in JAVS Viewer software (CVE-2024-4978) allows unauthorized PowerShell commands to be executed, leading to a supply-chain attack.
- In its latest updates, Google disclosed and patched four zero-day vulnerabilities in Chrome this month (CVE-2024-4947, CVE-2024-5274, CVE-2024-4671, and CVE-2024-4761) that were actively exploited by unnamed threat actors.
- Microsoft's Patch Tuesday for May 2024 patched two zero-day vulnerabilities (CVE-2024-30040 and CVE-2024-30051) in various versions of Microsoft Windows and Windows Exchange that unknown threat actors actively exploited. CVE-2024-30051 was exploited in malware attacks.

Detailed Analysis

Justice AV Solutions Backdoor Vulnerability (CVE-2024-4978) Exploited in Supply-Chain Attacks
Threat actors exploited a vulnerability tracked as CVE-2024-4978 in Justice AV Solutions (JAVS) Viewer software, leading to a supply-chain attack. This attack involved a backdoored version 8.3.7 of the JAVS Viewer installer, which allowed threat actors to gain full control of affected systems. Rapid7's investigation traced the infection to a malicious binary named `fffmpeg.exe`, linked to the GateDoor/Rustdoor malware family. The compromised installer, downloaded from the official JAVS website, facilitated unauthorized remote access.

Threat actors initiated the attack by distributing the malicious `JAVS Viewer Setup 8.3.7.250-1.exe` from the official JAVS website on March 5, 2024. Upon execution, the installer deployed the `fffmpeg.exe` binary, which ran encoded PowerShell scripts to establish remote access. These scripts bypassed security mechanisms and communicated with a command-and-control (C2) server to transmit host information and maintain a persistent connection. Additional malware binaries, such as `chrome_installer.exe` and `main.exe`, dropped Python scripts designed to scrape browser credentials. The compromised installer was signed with a certificate from "Vanguard Tech Limited", which differed from the legitimate Justice AV Solutions certificates, indicating unauthorized involvement in software distribution.

Google Patches High-Severity Vulnerability in Chrome Currently Exploited by Threat Actors
On May 9, 2024, Google patched a use-after-free vulnerability in the Google Chrome Visuals component, tracked as CVE-2024-4671, which is currently being exploited in the wild. Use-after-free vulnerabilities are flaws wherein a program attempts to use memory after it has been freed, leading to potential malicious outcomes such as data leakage, unauthorized code execution, or system crashes.

An anonymous researcher reported this high-severity vulnerability to Google. Google has not released technical details about the vulnerability to prevent further exploitation. Users of the Extended Stable channel will receive the fix in versions 124.0.6367.201/.202 for Mac and Windows and version 124.0.6367.201 for Linux.

Google Patches Third Actively Exploited Chrome Zero-Day Flaw (CVE-2024-4947) in May 2024
Google released an update on May 15, 2024, that addressed nine security vulnerabilities in its Chrome browser, including a critical zero-day vulnerability tracked as CVE-2024-4947. CVE-2024-4947 is a type confusion error in Chrome's V8 JavaScript and WebAssembly engine. The vulnerability enables threat actors to execute arbitrary code, cause the Chrome browser to crash or terminate, and perform unauthorized memory access. Google acknowledged that an unnamed threat actor is exploiting CVE-2024-4947 in the wild but did not provide additional details. Kaspersky security researchers Vasily Berdnikov and Boris Larin initially reported the existence of CVE-2024-4947 to Google. In a May 16, 2024, social media post, they said the vulnerability is "actively used in targeted attacks."

Google advised users to update to version 125.0.6422.60/.61 for Windows and macOS and version 125.0.6422.60 for Linux to prevent potential exploitation. The vulnerabilities patched by Google affect Chromium-based browsers such as Microsoft Edge, Brave, Opera, and Vivaldi.

Insikt Group has not identified additional information regarding malicious exploitation activity (including PoC exploits) targeting CVE-2024-4947 at the time of writing. However, CVE-2024-4947 is the third actively exploited zero-day that Google has patched since the beginning of May 2024

(the other two include CVE-2024-4671 and CVE-2024-4761). All three were disclosed and patched in less than a week.

CVE-2024-4947 is also the seventh Chrome zero-day that Google has patched since the beginning of 2024. All seven vulnerabilities are associated with in-the-wild exploitation activity. The four prior Chrome zero-days are as follows: CVE-2024-0519 (an out-of-bounds memory access flaw in Chrome's V8 JavaScript engine), CVE-2024-2887 (a type confusion vulnerability in Chrome's WebAssembly), CVE-2024-2886 (a use-after-free flaw affecting WebCodecs application programming interface [API]), and CVE-2024-3159 (an out-of-bounds read flaw in Chrome's V8 JavaScript engine).

Google Addresses Fourth Actively Exploited Chrome Zero-Day Flaw (CVE-2024-5274) in May 2024

Google released an emergency security update for the Chrome browser on May 23, 2024, to address an actively exploited zero-day vulnerability tracked as CVE-2024-5274. This is the fourth zero-day Google Chrome addressed in May 2024. The update addressed CVE-2024-5274 in version 125.0.6422.112/.113 for Windows and Mac and version 125.0.6422.112 for Linux. Google acknowledged that the vulnerability was being actively exploited but did not provide technical details. CVE-2024-5274 is a "type confusion" vulnerability found in Chrome's V8 JavaScript engine. This vulnerability mistakenly treats a piece of data as a different type, potentially leading to crashes, data corruption, and arbitrary code execution.

Microsoft Patches Two Actively Exploited Vulnerabilities in Patch Tuesday Update: CVE-2024-30040 and CVE-2024-30051

On May 14, 2024, Microsoft patched three zero-day vulnerabilities, two of which were actively exploited, among 61 security vulnerabilities in its May 2024 Patch Tuesday update. These vulnerabilities are as follows:

CVE-2024-30040 involves a security feature bypass in the Windows MSHTML platform that allows unauthenticated threat actors to execute arbitrary code by manipulating a malicious file without requiring the user to open it. As reported by BleepingComputer, the way in which the vulnerability was exploited and those who discovered it are unknown.

CVE-2024-30051 is an elevation of privilege vulnerability in the Windows Desktop Window Manager (DWM) Core Library. According to Kaspersky, threat actors exploited the vulnerability in phishing campaigns distributing Qakbot to gain SYSTEM privileges on compromised systems.

The updates included a fix for the publicly disclosed denial-of-service (DoS) flaw tracked as CVE-2024-30046 in Microsoft Visual Studio. Additionally, the updates addressed a critical remote code execution vulnerability in Microsoft SharePoint Server. Other vulnerabilities related to elevation of privilege, information disclosure, DoS, and spoofing were also addressed.

CVE Monthly Prominent Vulnerability Disclosures

This month, Insikt Group identified 258 vulnerabilities with high to very critical risk scores, per Recorded Future Intelligence Cloud data. Insikt Group provides the associated Risk Score, which ranges from "None" (0) to "Very Critical" (90-99). These scores continue to evolve with new analytics and sources.

In the table below, we listed fifteen of the highest-ranking vulnerabilities. Actively exploited vulnerabilities affecting the seven major software vendors are highlighted in gray.

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
1	CVE-2024-4978	99	Justice AV Solutions Viewer Setup	Justice AV Solutions Viewer Setup 8.3.7.250-1 contains a malicious binary that is signed with an unexpected authenticode signature. A remote, privileged threat actor may exploit this vulnerability to execute unauthorized PowerShell commands.	Yes
2	CVE-2024-4671	99	Various versions of Google Chrome	Use-after-free in Visuals in Google Chrome prior to 124.0.6367.201 allowed a remote attacker who had compromised the rendering process to potentially perform a sandbox escape via a crafted HTML page.	Yes
3	CVE-2024-4761	99	Various versions of Google Chrome	Out-of-bounds write in V8 in Google Chrome prior to 124.0.6367.207 allowed a remote attacker to perform an out-of-bounds memory write via a crafted HTML page.	Yes
4	CVE-2024-4947	99	Various versions of Google Chrome	Type confusion in V8 in Google Chrome prior to 125.0.6422.60 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	Yes

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
5	CVE-2024-5274	99	Various versions of Google Chrome	Type Confusion in V8 in Google Chrome prior to 125.0.6422.112 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	Yes
6	CVE-2024-30040	99	Microsoft Windows 10, Microsoft Windows Server 2019, Microsoft Windows Server 2016, Windows Server 2022, Microsoft Windows 10 1809, Microsoft Windows 10 21H2, Windows 11 21H2, Microsoft Windows 10 22H2, Microsoft Windows 11 22H2, Microsoft Windows 11 23H2, Microsoft Windows 10 1507, Microsoft Windows 10 1607	Windows MSHTML Platform Security Feature Bypass Vulnerability	Yes
7	CVE-2024-30051	99	Microsoft Windows 10, Microsoft Windows Server 2019, Microsoft Windows Server 2016, Windows Server 2022, Microsoft Windows 10 1809, Microsoft Windows 10 21H2, Windows 11 21H2, Microsoft Windows 10 22H2, Microsoft Windows 11 22H2, Microsoft Windows 11 23H2, Microsoft Windows 10 1507, Microsoft Windows 10 1607	Windows DWM Core Library Elevation of Privilege Vulnerability	Yes
8	CVE-2024-21793	79	BIG-IP Next Central Manager 20.0.1, BIG-IP Next Central Manager 20.1.0	An open data protocol (OData) injection vulnerability exists in the BIG-IP Next Central Manager API (uniform resource identifier [URI]).	No, but PoC exploit is available
9	CVE-2024-30046	79	Microsoft Visual Studio	Visual Studio Denial-of-Service Vulnerability	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
10	CVE-2024-29849	79	Veeam Backup Enterprise Manager	Veeam Backup Enterprise Manager allows unauthenticated users to log in as any user to the enterprise manager web interface.	No
11	CVE-2024-29895	79	Cacti 1.2.27	Cacti provides an operational monitoring and fault management framework. A command injection vulnerability on the 1.3.x DEV branch allows any unauthenticated user to execute arbitrary commands on the server when "`register_argc_argv`" option of PHP is "On".	No
12	CVE-2024-21683	79	Version 5.2 of Confluence Data Center and Server	This RCE (remote code execution) vulnerability, with a CVSS Score of 8.3, allows an authenticated attacker to execute arbitrary code. It has a high impact on confidentiality, integrity, and availability and requires no user interaction.	No, but PoC exploit is available
13	CVE-2024-24919	79	Check Point CloudGuard Network check versions r80 and r81	This vulnerability could allow an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote access virtual private network (VPN) or Mobile Access Software Blades. A security fix that mitigates this vulnerability is available.	No
14	CVE-2023-26009	76	Houzez Login Register plugin through 2.6.3.	Improper Privilege Management vulnerability in favethemes Houzez Login Register allows Privilege Escalation.	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
15	CVE-2024-22120	75	Zabbix Server	The Zabbix server can execute commands for configured scripts. After a command is executed, audit entry is added to "Audit Log". Due to the fact that the "clientip" field is not sanitized, it is possible to inject structured query language (SQL) into "clientip" and exploit time-based blind SQL injection.	No

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

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 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com