Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly August 2023

This report primarily analyzes the top vulnerabilities disclosed across 8 major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from August 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 August 2023, 2 confirmed zero-day vulnerabilities affected Microsoft and Ivanti products.
- In threat campaigns that attracted the highest attention from threat researchers, threat actors chained the exploitation of multiple vulnerabilities together to enable more severe effects.
- Microsoft patched 1 new zero-day vulnerability and released a Defense in Depth Update to fix a patch-bypass flaw affecting a vulnerability that was patched in July 2023 and previously exploited by RomCom to target guests of the July 2023 NATO Summit.
- 18 of the approximately 2,400 vulnerabilities disclosed in August 2023 were high-risk, according to Recorded Future data.

CVE Monthly Prominent Vulnerability Disclosures

We identified 18 newly disclosed vulnerabilities with high risk scores for August 2023, 2 of which were zero-day vulnerabilities affecting Microsoft and Ivanti products. Exploitation activity this month demonstrated that multiple medium-severity vulnerabilities can be exploited together to achieve the effects of 1 high-severity vulnerability; the actively exploited vulnerabilities that attracted some of the highest attention this month were chained together to enable attacks. First, threat actors exploited 4 vulnerabilities in Juniper Networks's Junos OS J-Web component to target Juniper EX switches and SRX firewalls. Each of the vulnerabilities has a medium-severity 5.3 CVSS score, but when aggregated, they have a collective high-severity CVSS score of 9.8; their exploitation can be chained together to enable remote code execution (RCE). In another instance of exploitation chaining, Ivanti urged its customers to patch CVE-2023-38035, an authentication bypass zero-day vulnerability affecting Sentry, a security product used to encrypt network traffic between mobile devices and enterprise servers. Threat actors chained exploitation of CVE-2023-38035 with the exploitation of 2 additional Ivanti Endpoint Manager Mobile (EPMM) vulnerabilities (CVE-2023-35078 and CVE-2023-35081) to enable their attacks.

While the actively exploited vulnerability spotlight was on Ivanti and Juniper Networks products this month, Microsoft continued to be the software vendor most consistently affected by actively exploited zero-day vulnerabilities, month-to-month. As part of its August 2023 Patch Tuesday, Microsoft patched 1 new actively exploited zero-day vulnerability (CVE-2023-38180) and released a Microsoft Office Defense-in-Depth Update to fix a patch-bypass flaw affecting CVE-2023-36884. The latter vulnerability, an RCE flaw affecting Microsoft Office, was patched in July 2023 and was previously exploited by RomCom to target guests of the July 2023 NATO Summit.

Threat Actors Attempt to Exploit Recently Patched Vulnerabilities in Juniper Networks's J-Web to Target Juniper EX Switches and SRX Firewalls

The Shadowserver Foundation reported that starting on August 25, 2023, it observed threat actors attempting to exploit 4 recently patched vulnerabilities to target Juniper EX switches and SRX firewalls. That same day, watchTowr Labs published proof of concept (PoC) exploit code for the vulnerabilities. The 4 vulnerabilities collectively represent 2 bugs found in the J-Web component of Juniper Networks's Junos OS, which powers both Juniper EX switches and SRX firewalls. J-Web is "the web-based UI that can be used to configure the [Juniper EX switches and SRX firewalls]" in lieu of using command-line interface (CLI).

Shadowserver CEO Piotr Kijewski told BleepingComputer that the attackers appear to be using exploits that are inspired by — but not identical to — watchTowr's published PoC exploit code. As Kijewski noted, "Based on our honeypot observations, I would say all Juniper instances with J-Web exposed have already been hit. 29 IPs [are] currently attempting these attacks, possibly [representing] multiple threat actors". According to August 29, 2023, Shadowserver data, approximately 8,200 J-Web instances remain exposed to the internet. A majority of the exposed instances were located in Asia (5,262), followed by North America (1,258), Europe (1,057), South America (450), Africa (155), and Oceania (79). By specific countries, a majority of exposed J-Web instances are located in South Korea (~3,000), followed by the US (857), Hong Kong (372), Indonesia (317), and Turkey (242). Shadowserver did not provide any information or statistics about instances in which the J-Web vulnerabilities were successfully exploited to compromise Juniper EX switches and SRX firewalls.

Each of the vulnerabilities affecting J-Web has a medium-severity 5.3 CVSS score, but when aggregated, the vulnerabilities are assigned a collective high-severity CVSS score of 9.8. Juniper Networks assessed that by "chaining exploitation of these vulnerabilities, an unauthenticated, network-based attacker may be able to remotely execute code on [Juniper EX switches and SRX firewalls]". Juniper Networks patched and provided workarounds and mitigation suggestions for the vulnerabilities in an August 17, 2023, out-of-cycle security bulletin.

Although we have verification that threat actors are attempting to exploit Juniper Networks's J-Web vulnerabilities, there is currently no verification that any of this exploitation activity has resulted in a successful attack on and compromise of any enterprises that use EX switches and SRX firewalls. However, the threat actors responsible for the exploitation attempts appear to be adaptable, as their exploits resemble but are not identical to the PoC exploit code published by watchTowr. Therefore, well-resourced threat actors may be able to eventually tailor their exploits to enable a successful attack.

To avoid being a victim of such an attack, affected organizations are urged to view Juniper Networks's security bulletin and apply all relevant patches immediately. For those organizations that are unable to apply a patch immediately, Juniper Networks provided the following workaround: "disable J-Web or limit access to only trusted hosts".

Juniper networks provided the following descriptions for each vulnerability:
CVE-2023-36844: A PHP External Variable Modification vulnerability in J-Web of Juniper Networks Junos OS on EX Series allows an unauthenticated, network-based attacker to control certain, important environment variables.
CVE-2023-36845: A PHP External Variable Modification vulnerability in J-Web of Juniper Networks Junos OS on EX Series and SRX Series allows an unauthenticated, network-based attacker to control certain important environment variables.
CVE-2023-36846: A Missing Authentication for Critical Function vulnerability in Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause limited impact to the file system integrity.
CVE-2023-36847: A Missing Authentication for Critical Function vulnerability in Juniper Networks Junos OS on EX Series allows an unauthenticated, network-based attacker to cause limited impact to the file system integrity.

Ivanti Warns of Actively Exploited Zero-Day Vulnerability CVE-2023-38035 in Sentry Product
IT software company Ivanti warned customers in an August 21, 2023, security advisory about a new, critical, authentication-bypass zero-day vulnerability, tracked as CVE-2023-38035, affecting its

Sentry (formerly known as MobileIron Sentry) security product. Ivanti Sentry provides gateway security by encrypting network traffic between mobile devices and enterprise servers. Ivanti revealed in its advisory that threat actors are actively exploiting the vulnerability in the wild and that the exploitation affected a "very limited number of customers".

Ivanti said it has been informed by an unknown source that CVE-2023-38035 was chained together with 2 previously disclosed vulnerabilities affecting Ivanti's Endpoint Manager Mobile (EPMM), tracked as CVE-2023-35078 (an authentication bypass flaw) and CVE-2023-35081 (a vulnerability that enables arbitrary file-write). CVE-2023-35078 and CVE-2023-35081 were patched in July 2023.

Per Ivanti's recent advisory, CVE-2023-38035 exists in the administrator portal in Ivanti Sentry. Successful exploitation of the flaw may allow a threat actor to bypass authentication mechanisms because of insufficient security restrictions in an Apache configuration. As a result, threat actors may alter configurations, run malicious commands, and modify files within affected systems. The vulnerability affects versions 9.18., 9.17, and 9.16, including older versions. Products not affected by the vulnerability are Ivanti Endpoint Manager Mobile (EMM), MobileIron Cloud, and Ivanti Neurons for Mobile Device Management (MDM).

Ivanti urged customers to disconnect MICS (MobileIron Core Service) from the internet and has provided customized scripts to address the issue based on specific software versions. Ivanti encouraged customers to apply the security patch to prevent potential exploitation from malicious actors.

Microsoft Fixes Patch Bypass Flaw for Vulnerability Previously Exploited by RomCom to Target NATO Summit Guests; Patches 1 Additional Zero-Day

As part of its August 2023 Patch Tuesday report, Microsoft released 87 software fixes, including updates to remediate 2 zero-day vulnerabilities, CVE-2023-36884 and CVE-2023-38180; CVE-2023-36884 is an RCE flaw affecting Microsoft Office that was previously exploited by RomCom to target guests of the July 2023 NATO Summit. RomCom, also known as Storm-0978, is known to engage in both ransomware and intelligence operations. CVE-2023-38180 is a denial-of-service (DoS) vulnerability affecting .NET applications and Visual Studio. Microsoft did not release any additional data about how CVE-2023-38180 was exploited in the wild.

CVE-2023-36884 was previously patched in July 2023; for August 2023, Microsoft released a Microsoft Office Defense in Depth Update (ADV230003) to fix a patch bypass flaw affecting CVE-2023-36884. Microsoft noted in the update that the "defense in depth update is not a vulnerability update, but installing this update stops the attack chain leading to the Windows Search Remote Code Execution Vulnerability (CVE-2023-36884)". Exploitation of CVE-2023-36884 enables threat actors to create Microsoft Office documents that could bypass the Mark-of-the-Web (MoTW) security feature. When CVE-2023-36884 is exploited as an initial access vector in phishing campaigns, malicious attachments can be opened and executed by the victim without triggering a security warning.

As instructed by Microsoft, affected organizations should apply all patches and updates immediately, with priority given to applying the Microsoft Office Defense in Depth Update ADV230003 — which fixes the patch-bypass flaw created by the initial July patch of CVE-2023-36884 — and to patching CVE-2023-38180.

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	Malware	Zero-Day
1	CVE-2023-38180	99	Microsoft .NET Framework & Visual Studio	DoS vulnerability in Kestrel web server for ASP.NET Core	N/A	Yes
2	CVE-2023-38035	99	Ivanti Sentry	Authentication bypass vulnerability in MobileIron Core (MICS) admin portal	N/A	Yes
3	CVE-2023-35081	99	Ivanti Endpoint Manager Mobile (EPMM)	Path traversal vulnerability in Ivanti EPMM application	N/A	No
4	CVE-2023-35082	99	Ivanti Endpoint Manager Mobile (EPMM)	Authentication bypass vulnerability in Ivanti EPMM application	N/A	No
5	CVE-2023-35386	94	Microsoft Windows 10, 11, Server	Elevation of privilege vulnerability in Windows Kernel	N/A	No
6	CVE-2023-36900	93	Microsoft Windows 10, 11, Server	Elevation of privilege vulnerability in Windows Common Log File System Driver	N/A	No
7	CVE-2022-40982	79	Intel Core Intel Microcode Intel Xeon Firmware Cisco IOS Debian Linux Red Hat Enterprise Linux	Information exposure vulnerability in some Intel processors	N/A	No
8	CVE-2023-36844	79	Juniper Networks EX ethernet switches	PHP external variable modification vulnerability in J-Web of Juniper Networks Junos OS	N/A	No
9	CVE-2023-36845	79	Juniper Networks EX ethernet switches, SRX firewalls	PHP external variable modification vulnerability in J-Web of Juniper Networks Junos OS	N/A	No
10	CVE-2023-36846	79	Juniper Networks SRX firewalls	Missing authentication for	N/A	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/ Component	Malware	Zero-Day
				critical function vulnerability in Junos OS		
11	CVE-2023-36847	79	Juniper Networks EX ethernet switches	Missing authentication for critical function vulnerability in Junos OS	N/A	No
12	CVE-2023-39143	79	PaperCut NG & MF print management software	Path traversal vulnerability affecting PaperCut NG and MF	N/A	No
13	CVE-2023-32560	76	Ivanti Avalanche	An arbitrary code execution vulnerability in Wavelink Avalanche Manager	N/A	No
14	CVE-2023-33241	76	Crypto wallets that use GG18 or GG20 TSS protocol	Improper neutralization of special elements in output used by a downstream component in GG18 or GG20 TSS protocol	N/A	No
15	CVE-2023-29468	75	Texas Instruments (TI)	Buffer overflow vulnerability in WiLink WL18xx MCP driver	N/A	No
16	CVE-2023-20562	75	Advanced Micro Devices (AMD) AMD uProf	Insufficient validation vulnerability in the IOCTL (Input Output Control) input buffer of AMD uProf	N/A	No
17	CVE-2022-48603	75	ScienceLogic SL1	SQL injection vulnerability in the “message viewer iframe” feature of the ScienceLogic SL1	N/A	No
18	CVE-2022-48602	75	ScienceLogic SL1	SQL injection vulnerability exists in the “message viewer print” feature of the ScienceLogic SL1	N/A	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.