Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly February 2024

This report primarily analyzes the top vulnerabilities disclosed across eight major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from February 1 to 29, 2024. 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 February 2024, twelve newly disclosed, actively exploited vulnerabilities affected Fortinet, Microsoft, Ivanti, Mastodon, and ConnectWise.
- Eighteen of the approximately 2,400 vulnerabilities disclosed in February 2024 were high-risk, according to Recorded Future data.
- Nine of the eighteen high-risk vulnerabilities affected Microsoft and Fortinet products.
- Various vulnerabilities found in public-facing applications, including ConnectWise ScreenConnect, WordPress, Microsoft Outlook, and Oracle Weblogic, continued to enable threat actors to execute Remote Code Execution (RCE) attacks this month.

CVE Monthly Prominent Vulnerability Disclosures

In February 2024, we identified eighteen high-risk vulnerabilities, twelve of which are known to be exploited in the wild and should be prioritized for remediation. More details on each of these vulnerabilities are provided below.

According to data from the Recorded Future Intelligence Cloud, the top three trending vulnerabilities associated with current threat activity are listed below:

- CVE-2024-21412: a security feature bypass vulnerability in Microsoft Defender SmartScreen that allowed threat actors to infect victims with DarkMe malware.
- CVE-2024-21893: A server-side request forgery vulnerability in the Security Assertion Markup Language (SAML) component of Ivanti Connect Secure virtual private network (VPN) that, if exploited, allows an attacker to access certain restricted resources without authentication.
- CVE-2024-21413: A critical RCE vulnerability in Microsoft Outlook that, if exploited, enables unauthorized Windows NTLM credential theft and arbitrary code execution without user interaction.

In February 2024, there was a series of sophisticated cyberattacks exploiting zero-day vulnerabilities. The advanced persistent threat (APT) group Water Hydra exploited a Microsoft Defender SmartScreen bypass vulnerability (CVE-2024-21412) to target financial traders with the DarkMe remote access trojan (RAT). Additionally, China-linked APT group UNC5221 exploited vulnerabilities in Ivanti Connect Secure VPNs (CVE-2023-46805 and CVE-2024-21887) in an espionage campaign affecting a wide array of sectors globally.

In addition to exploiting zero-day vulnerabilities, threat actors also exploited known and previously patched vulnerabilities this month. Akira Ransomware Group exploited an older vulnerability in Cisco AnyConnect (CVE-2020-3259) for data theft, and a new variant of the FritzFrog botnet targeted unpatched internal networks by exploiting the Log4Shell vulnerability (CVE-2021-44228). Collectively, these incidents underscore the necessity for defensive strategies, timely patch management, and threat intelligence to mitigate cyber threats.

Lazarus Group Develops Windows Kernel Elevation of Privilege (CVE-2024-21338) Exploit, Updated Rootkit

The Lazarus Group exploited a privilege escalation vulnerability in the Windows driver `appid.sys` AppLocker using an updated version of its FudModule rootkit, according to reporting from Avast published on February 28, 2024. For reference, AppLocker is a whitelisting technology within Windows whose set policies to accept apps are enforced by `appid.sys`. The vulnerability, CVE-2024-21338, was patched in Microsoft's February Patch Tuesday release.

The vulnerability is exploited by tricking `appid.sys` driver's Input and Output Control (IOCTL) dispatcher to call an arbitrary pointer and thus allow the execution of code, subsequently bypassing security checks that would otherwise be in place. FudModule is responsible for disabling security software and is an updated version of FudModule rootkits identified in September 2022.

By exploiting the vulnerability and using FudModule, Lazarus Group gained kernel-level access to Windows machines and disabled security software, such as Microsoft Defender, Crowdstrike Falcon, and AhnLab V3 Endpoint Security. Notably, Lazarus Group was able to cross the administrator-to-kernel boundary using the updated FudModule and achieve read and write access to victim machines, including the ability to conceal their malware within the kernel. Typically, the administrator-to-kernel boundary is serviced by Microsoft as a security issue.

Avast concluded that Lazarus Group primarily sought to gain persistent access to victim machines while remaining undiscovered. The company also stated it believed that the group is continuing to update FudModule with a focus on kernel exploitation. In previous attacks, for instance, Lazarus Group employed much noisier "Bring Your Own Vulnerable Driver" techniques to cross the administrator-to-kernel boundary, with FudModule's newly observed capability providing the group with a more versatile and effective tool to achieve the same goal.

ScreenConnect Vulnerabilities Exploited to Deploy LockBit Ransomware

On February 23, 2024, Sophos reported that threat actors exploited authentication bypass and path traversal vulnerabilities in ConnectWise ScreenConnect (ConnectWise Control) servers. The attacks targeted government and healthcare organizations and ultimately led to the deployment of LockBit ransomware. The vulnerabilities, CVE-2024-1709 and CVE-2024-1708, impact older versions of ScreenConnect and have been mitigated in version 23.9.8 and later. Sophos X-Ops observed active exploitation of these vulnerabilities, prompting ConnectWise to release security updates and remove license restrictions for customers to upgrade to the latest software version.

Microsoft Patches CVE-2024-21413: Critical Outlook Vulnerability Leads to Exposed NTLM Credentials and Remote Code Execution

On February 14, 2024, Checkpoint Research identified a critical vulnerability in Microsoft Outlook, tracked as CVE-2024-21413 and dubbed #MonikerLink. This vulnerability, which has reportedly been exploited in the wild, allows for both the theft of Windows Network Lan Module (NTLM) credentials and the execution of arbitrary code without user interaction. The vulnerability exploits a method by which modified hyperlinks in emails, specifically those appended with an exclamation mark and additional text, can circumvent Outlook's security protocols and Microsoft Word's Protected View.

CVE-2024-21413 arises due to the misuse of the Windows MkParseDisplayName application programming interface (API), potentially affecting other applications that rely on this API. The manipulated hyperlinks use the `file://` protocol, directing victims to threat actor-controlled servers. When such a link is clicked, Outlook fails to issue warnings or block access, potentially leading to unauthorized access and code execution.

Microsoft released a security update addressing CVE-2024-21413.

Microsoft Identifies Exploitation of CVE-2024-21410 Vulnerability Within Microsoft Exchange Server

On February 14, 2024, Microsoft patched a privilege escalation vulnerability in Microsoft Exchange Server, tracked as CVE-2024-21410. Microsoft did not provide specific details about the attacks but stated that threat actors could exploit CVE-2024-21410 by manipulating the NT LAN Manager (NTLM) credentials-leaking flaw in a client such as Outlook. By compromising these credentials, threat actors can conduct NTLM relay attacks on the Microsoft Exchange Server to gain elevated privileges. Threat actors conduct NLTM relay attacks by coercing server authentication against a maliciously controlled NTLM relay server, enabling them to impersonate users and escalate privileges.

Microsoft recommended using Exchange Server 2019 CU14 for fortified security with NTLM credentials Relay Protections. This update enhances Windows Server authentication, delivering robust protection against relay and man-in-the-middle attacks.

Water Hydra Exploits Microsoft Defender SmartScreen Bypass Vulnerability, CVE-2024-21412, to Target Finance Traders

On February 13, 2024, Trend Micro reported that the APT group Water Hydra, also known as DarkCasino, has been exploiting a zero-day vulnerability tracked as CVE-2024-21412 in Microsoft Defender SmartScreen in their campaigns targeting financial market traders. Per Trend Micro, Water Hydra has been using CVE-2024-21412 in its campaigns since late December 2023. The group exploited the vulnerability to bypass Microsoft Defender SmartScreen and infect victims with the DarkMe remote access trojan (RAT).

For initial access, Water Hydra used spearphishing messages on forex trading forums and stock trading Telegram channels to lure victims into infecting their devices with DarkMe. They used various social engineering techniques that involved using a stock chart that redirected to a malicious URL, *fxbulls[.]ru*, which posed as a legitimate forex broker website, *fxbulls[.]com.*

Unique to the attack chain, Trend Micro's Zero Day Initiative (ZDI) found that one of the internet shortcuts used as the initial access vector pointed to a second internet shortcut, bypassing the patch for CVE-2023-36025. This exploit, tracked as CVE-2024-21412, has since been patched by Microsoft. A full list of indicators of compromise (IoCs) can be found in Trend Micro's report.

Threat Actors Exploit Ivanti Zero-Day Flaw CVE-2024-21893 to Inject DSLog Backdoor on Target Systems

On February 12, 2024, Orange Cyberdefense reported that threat actors exploited a Server-Side Request Forgery (SSRF) vulnerability tracked as CVE-2024-21893, which affects Ivanti appliances. Threat actors exploited the vulnerability as a zero-day and injected a new backdoor, tracked as DSLog, on target systems. Per Orange Cyberdefense, successful exploitation of the vulnerability allows unauthenticated, remote access and command execution with high privileges on compromised devices. DSLog backdoor allowed threat actors persistent access to compromised devices. Ivanti released patches for CVE-2024-21893 and four other vulnerabilities on January 31, 2024. On February 3, 2024, Orange Cyberdefense identified approximately 670 devices, systems, or network components that were compromised as a result of attacks exploiting CVE-2024-21893.

After establishing a foothold in a target system, the threat actors used encoded commands embedded in the RetrievalMethod uniform resource identifier (URI) section of SAML authentication requests to perform reconnaissance and confirm root access. This allowed threat actors to exploit normal authentication processes to avoid detection. Once the DSLog backdoor is executed, it proceeds to exfiltrate data, move laterally within the system, and deploy additional malicious payloads, including

ransomware. The threat actors used fake SAML requests that enabled the backdoor to bypass security tools and potentially facilitate information theft campaigns and system disruptions.

Fortinet Warns Likely Exploitation of SSL VPN Vulnerability CVE-2024-21762
On February 8, 2024, FortiGuard Labs issued a warning regarding a critical RCE vulnerability in FortiOS Secure Sockets Layer (SSL) VPN identified as CVE-2024-21762, which is "potentially" being exploited in the wild. This vulnerability is an out-of-bounds write issue that can be triggered by remote, unauthenticated attackers through HTTP requests. Affected versions range across FortiOS 6.0 through 7.4, with patches available for each version.

In parallel, Fortinet has disclosed other vulnerabilities, including CVE-2024-23113, alongside CVE-2024-21762, though CVE-2024-21762 remains a focal point in this report due to its potential active exploitation and high severity. Fortinet's devices have been a consistent target for threat actors, with past incidents involving ransomware attacks and cyber espionage. An example includes the COATHANGER malware deployed by Chinese state-sponsored actors targeting FortiOS vulnerabilities, demonstrating the strategic interest in exploiting Fortinet vulnerabilities for attacks.

Mastodon Addresses CVE-2024-23832 Vulnerability in User Accounts
On February 2, 2024, Mastodon, an open-source social networking platform, patched a remote user impersonation and account takeover vulnerability, tracked as CVE-2024-23832, affecting its user accounts. This vulnerability stems from insufficient validation of source authenticity in Mastodon. If exploited, CVE-2024-23832 could enable threat actors to masquerade as users, resulting in the compromise of their remote accounts. The affected Mastodon versions are those prior to 3.5.17, 4.0.13, 4.1.13, and 4.2.5.

CVE Monthly Prominent Vulnerability Disclosures

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

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
1	**CVE-2024-21412**	99	Microsoft Windows Server	A security feature bypass vulnerability in Microsoft Defender SmartScreen that allowed threat actors to infect victims with DarkMe malware.	Yes
2	**CVE-2024-21762**	99	Fortinet FortiOS SSL VPN	RCE vulnerability. This vulnerability is an out-of-bounds write issue that can be triggered by remote unauthenticated attackers through HTTP requests.	Yes
3	**CVE-2024-21338**	99	Windows Driver	Privilege escalation vulnerability. The vulnerability is specifically exploited by tricking `appid.sys` driver's Input and Output Control (IOCTL) dispatcher to call an arbitrary pointer and thus allow the execution of code, subsequently bypassing security checks that would otherwise be in place.	Yes
4	**CVE-2024-21351**	99	Microsoft Windows	RCE vulnerability.	Yes
5	**CVE-2024-21413**	99	Microsoft Outlook	This vulnerability allows for both the theft of Windows NTLM credentials and the execution of arbitrary code without user interaction.	Yes
6	**CVE-2024-21410**	99	Microsoft Exchange Server	Privilege escalation vulnerability. Threat actors can exploit CVE-2024-21410 by manipulating the NT LAN Manager (NTLM) credentials-leaking flaw in a client such as Outlook. By compromising these credentials, threat actors can conduct NTLM relay attacks on the Microsoft Exchange Server to gain elevated privileges.	Yes
7	**CVE-2024-1709**	99	ConnectWise ScreenConnect	Bypass authentication vulnerability.	Yes
8	**CVE-2024-1708**	99	ConnectWise ScreenConnect	Path traversal vulnerability.	Yes
9	**CVE-2024-23832**	99	Mastodon	A remote user impersonation and account takeover vulnerability.	Yes
10	**CVE-2024-21893**	89	Ivant Connect Secure and Policy Secure	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure VPN that, if exploited, allows an attacker to access certain restricted resources without authentication.	Yes
11	**CVE-2024-23109**	79	Fortinet FortiSIEM	Improper neutralization of special elements flaw used in an operating system (OS) command ("OS command injection") that allows a threat actor to execute unauthorized code or commands via crafted API requests in certain Fortinet FortiSIEM versions.	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
12	**CVE-2024-23108**	79	Fortinet FortiSIEM	Improper neutralization of special elements flaw used in an OS command ("OS command injection") that allows a threat actor to execute unauthorized code or commands via crafted API requests in certain Fortinet FortiSIEM versions.	No
13	**CVE-2024-23113**	79	Fortinet FortiOS	RCE vulnerability that stems from a format string flow in FortiOS fgfmd daemon that allows threat actors to craft malicious requests.	Yes
14	**CVE-2024-20931**	79	Oracle Weblogic Server	An RCE vulnerability affecting Oracle Weblogic Server (WLS). It is a Java Naming and Directory Interface (JNDI) injection bug that allows threat actors to remotely execute malicious commands on a vulnerable system.	No
15	**CVE-2024-22024**	79	Ivanti Connect Security, Policy Secure, and ZTA gateway	Authentication bypass vulnerability. The flaw is an XML external entity (XXE) vulnerability in the SAML component that could allow threat actors to access restricted resources without authentication.	Yes
16	**CVE-2024-22245**	79	VMware Enhanced Authentication Plug-in (EAP)	An arbitrary authentication relay vulnerability that, if exploited, threat actors can use to relay Kerberos service tickets and hijack privileged EAP sessions.	No
17	**CVE-2023-50386**	78	Apache Solr	RCE vulnerability. The vulnerability involves inadequate control over dynamically managed code resources, allowing unrestricted upload of potentially dangerous file types through the ConfigSets API. This flaw could enable uploaded Java jar and class files to be saved and potentially executed if backups were stored in directories included in Solr's ClassPath or ClassLoaders, posing a risk, especially when Solr's Authorization is not enabled.	No
18	**CVE-2024-23313**	76	Libbiosig, an open-source library processing medical signal data	Arbitrary code execution vulnerability.	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.