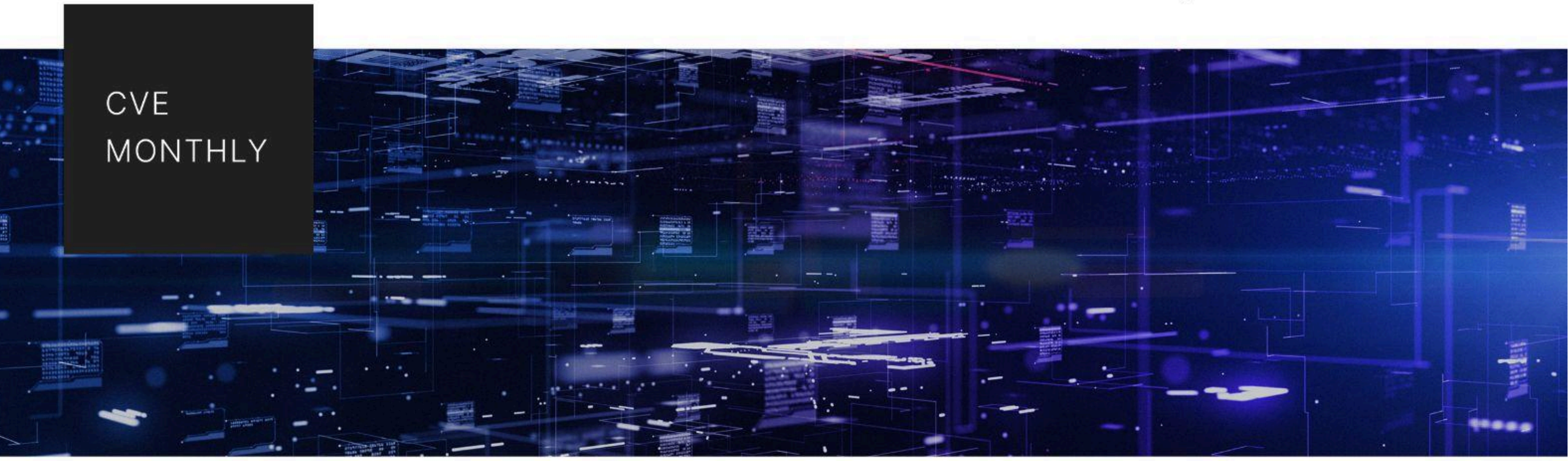
CVE
MONTHLY



Recorded Future CVE Monthly March 2024

Executive Summary

In March 2024, we identified nine high-risk vulnerabilities, four of which are known to be exploited in the wild and should be prioritized for remediation.

The most concerning vulnerability trend in March 2024 involved the active exploitation of critical vulnerabilities after third-party security researchers published proof of concepts (PoCs) for these vulnerabilities, independent of the vendors who maintain and patch them. In early March 2024, JetBrains silently patched two high-risk vulnerabilities, CVE-2024-27198 and CVE-2024-27199, in its TeamCity continuous integration and continuous delivery/deployment (CI/CD) servers. Just five hours later, Rapid7 independently published PoC exploit code for the vulnerabilities on March 4, 2024, after which reports emerged that threat actors were actively exploiting CVE-2024-27198 and CVE-2024-27199 to deploy ransomware. JetBrains blamed Rapid7's disclosure of the PoC codes for the compromise of several of its customers' TeamCity servers. Rapid7 and JetBrains' disclosure policies for the vulnerabilities were at odds, with JetBrains maintaining policies in support of silent patching and Rapid7 maintaining policies favoring greater transparency.

In a similar instance, on March 12, 2024, Fortinet addressed a critical SQL injection vulnerability tracked as CVE-2023-48788 in its FortiClient Endpoint Management Server (EMS) software. On March 21, 2024, Horizon3 independently published PoC exploit code for CVE-2023-48788 and on March 25, 2024, the US Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2023-48788 to its Known Exploited Vulnerabilities Catalog (KEV).

The active exploitation of newly patched vulnerabilities after the release of PoC exploit code in March 2024 highlights the ongoing tension and debate within the security community regarding ideal methods for disclosing and patching vulnerabilities. JetBrains maintains that its decision to initially release silent patches was an effort to make patch analysis harder for attackers and give its customers a buffer of time to implement the patches. Rapid7 maintains that its policy against silent patching centers on the fact that silent patches leave defenders in the dark while allowing attackers to reverse-engineer patches and develop their own PoC code. JetBrains argued that the information contained within Rapid7's PoC code enabled low-skill threat actors to effectively exploit the tool, whereas withholding the details of the vulnerabilities would have limited the exploitation of the vulnerabilities to a few high-skill threat actors.

Given the typical lag times between enterprise software patch release and actual deployment on enterprise systems, there is merit to JetBrains's argument against Rapid7's immediate release of PoC exploit code. While enterprises struggle to find and implement real-time patch deployment solutions, releasing PoC exploit code within hours of vulnerability disclosure likely proves more advantageous to threat actors than defenders. While security researchers continue to debate the best approach to vulnerability disclosure, these instances of active exploitation after the release of PoC code are likely to continue, driving enterprises toward adopting technology that better supports real-time patch deployment.

Key Findings

- In March 2024, four newly disclosed, actively exploited vulnerabilities affected JetBrains TeamCity, various Apple products, and FortiClient Endpoint Management Server (EMS) software.
- Three high-risk vulnerabilities were actively exploited after third parties, independent of affected software vendors, disclosed PoC exploit code. This highlights ongoing tension and debate within the security community about the best approach to vulnerability disclosure from a defender's perspective.
- JetBrains blamed Rapid7's disclosure of PoC code for the active exploitation of two newly disclosed, high-risk TeamCity vulnerabilities, CVE-2024-27198 and CVE-2024-27199. Rapid7 published the PoC code just five hours after JetBrains released patches for the vulnerabilities.
- Nine of the approximately 2,500 vulnerabilities disclosed in March 2024 were high-risk, according to Recorded Future data.

Detailed Analysis

JetBrains TeamCity Vulnerabilities CVE-2024-27198 and CVE-2024-27199 Used to Deploy Multiple Malware

On March 3, 2024, JetBrains patched and disclosed two high-risk vulnerabilities, CVE-2024-27198 and CVE-2024-27199, in JetBrains TeamCity continuous integration and continuous delivery/deployment (CI/CD) servers. The flaws enable "an unauthenticated attacker with HTTP(S) access to a TeamCity server to bypass the authentication checks and gain administrative control of the TeamCity server". The vulnerabilities were patched with JetBrains's release of TeamCity version 2023.11.4.

Rapid7 discovered the vulnerabilities in February 2024, reported them to JetBrains on an undisclosed date, and published proof-of-concept (PoC) code for the vulnerabilities on March 4, 2024. Later, on March 19, 2024, Trend Micro reported that unspecified threat actors exploited the vulnerabilities to deploy Jasmin Ransomware, cryptocurrency miners, and other malware on compromised systems.

CVE-2024-27198 has a CVSS score of 9.8 and allows remote code execution (RCE) through an authentication bypass in TeamCity's web component. Attackers send a specially crafted HTTP request to generate a 404 response, then manipulate the HTTP query string and path parameter to bypass authentication and execute code remotely. CVE-2024-27199, on the other hand, involves directory traversal, enabling attackers to access restricted directories and files, potentially leading to information leakage and modification of system settings.

Fortinet Patched Actively Exploited Critical RCE Vulnerability CVE-2023-48788 in its FortiClient Enterprise Management Server

On March 12, 2024, Fortinet addressed an actively exploited critical SQL injection vulnerability tracked as CVE-2023-48788 in its FortiClient Endpoint Management Server (EMS) software, affecting versions 7.0 and 7.2. This flaw enables threat actors to gain RCE on vulnerable servers with SYSTEM privileges, without requiring user interaction. CVE-2023-48788 resides in the DB2 Administration Server (DAS) component of the FortiClient EMS, which is essential for managing endpoints connected to an enterprise network. FortiClient EMS facilitates the deployment of FortiClient software and the assignment of security profiles on Windows devices.

Horizon3's Attack Team confirmed the vulnerability's critical severity and released PoC exploit code for it on March 21, 2024. On March 25, 2024, CISA added CVE-2023-48788 to its KEV, confirming its active exploitation.

Apple Emergency Patch Addresses Two Actively Exploited Vulnerabilities, CVE-2024-23225 (iOS kernel) and CVE-2024-23296 (RTKit)

On March 5, 2024, Apple released iOS 17.4 and iPadOS 17.4 emergency patches addressing critical zero-day vulnerabilities, CVE-2024-23225 (iOS kernel) and CVE-2024-23296 (RTKit). If exploited, both vulnerabilities allow threat actors with arbitrary kernel read and write capabilities to bypass kernel memory protections. Apple stated that CVE-2024-23225 and CVE-2024-23296 “may have been” exploited in the wild but did not further elaborate on these reports. The security patch is available for the following affected devices:

- iPhone XS and later models
- iPad Pro 12.9-inch 2nd generation and later models
- iPad Pro 10.5-inch
- iPad Pro 11-inch 1st generation and later models
- iPad Air 3rd generation and later models
- iPad 6th generation and later models
- iPad mini 5th generation and later models

CVE Monthly Prominent Vulnerability Disclosures

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
1	CVE-2024-27198	99	JetBrains TeamCity	In JetBrains TeamCity before 2023.11.4, this vulnerability enables authentication bypass allowing attackers to perform administrative actions.	Yes
2	CVE-2024-23225	99	Apple iPad OS, WatchOS, iPhone OS, macOS, tvOS, watchOS	A memory corruption issue was addressed with improved validation. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. This issue is fixed in iOS 16.7.6, iPadOS 16.7.6, iOS 17.4, and iPadOS 17.4.	Yes
3	CVE-2024-23296	99	Apple iPad OS, WatchOS, iPhone OS, macOS, tvOS, watchOS	A memory corruption issue was addressed with improved validation. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited. This issue is fixed in iOS 17.4 and iPadOS 17.4.	Yes
4	CVE-2023-48788	99	Fortinet FortiClient Enterprise Management Server (EMS)	An improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2 and FortiClientEMS 7.0.1 through 7.0.10 allows an attacker to execute unauthorized code or commands via specially crafted packets.	Yes
5	CVE-2024-21899	79	QNAP QTS	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. The issue is fixed in the following versions: QTS 5.1.3.2578 build 20231110 and later, QTS 4.5.4.2627 build 20231225 and later, QuTS hero h5.1.3.2578 build 20231110 and later, QuTS hero h4.5.4.2626 build 20231225 and later, and QuTScloud c5.1.5.2651 and later.	No
6	CVE-2024-27199	79	JetBrains TeamCity	In JetBrains TeamCity before 2023.11.4, this vulnerability enables path traversal allowing attackers to perform administrative actions.	Yes
7	CVE-2024-22252	79	VMware ESXi VMware Fusion VMware Workstation	VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox, whereas on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
				is installed.	
8	CVE-2023-41724	76	Ivanti Standalone Sentry	A command injection vulnerability in Ivanti Sentry prior to 9.19.0 allows an unauthenticated threat actor to execute arbitrary commands on the underlying operating system of the appliance within the same physical or logical network.	No
9	CVE-2024-22253	75	VMware ESXi VMware FusionVMware Workstation	VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the UHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox, whereas on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.	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.