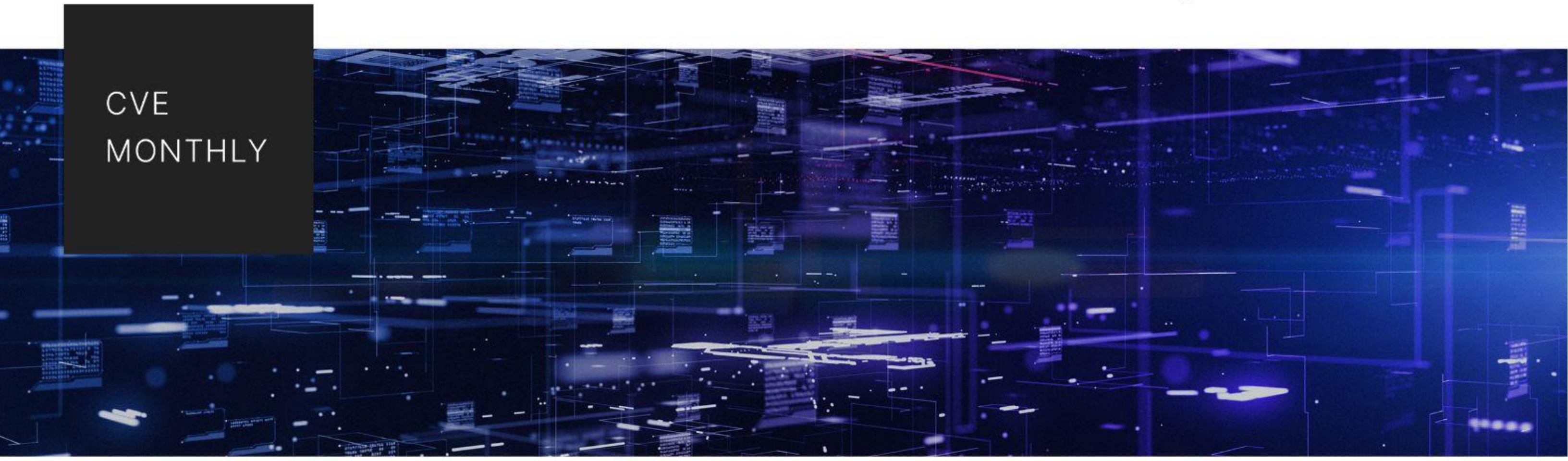
Recorded Future®

CVE
MONTHLY



Recorded Future CVE Monthly October 2023

This report primarily analyzes the top vulnerabilities disclosed across 8 major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from October 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 October 2023, 9 high-risk zero-day vulnerabilities affected Apple, Microsoft, Apache, F5, and all vendors that use the HTTP/2 protocol and the GNU C Library.
- Security researchers are observing successful, ongoing mass exploitation of “Citrix Bleed” or CVE-2023-4966, a zero-day vulnerability affecting Citrix NetScaler ADC and NetScaler Gateway devices. The exploitation of CVE-2023-4966, first observed in late August 2023, is enabling various threat actors’ stealthy, persistent access to enterprise environments for ransomware deployment and more.
- A zero-day vulnerability (CVE-2023-44487) affecting the HTTP/2 protocol was exploited to enable unprecedentedly large-scale Layer 7 distributed denial-of-service (DDoS) attacks on Google, Amazon Web Services (AWS), and Cloudflare. HTTP/2 protocol is used for approximately 40% of websites globally, so the CVE-2023-44487 vulnerability and the DDoS attack vector it enables have broad implications for all vendors providing web services.
- 16 of the approximately 2,500 vulnerabilities disclosed in October 2023 were high-risk, according to Recorded Future data.

CVE Monthly Prominent Vulnerability Disclosures

We identified 16 newly disclosed vulnerabilities with high risk scores for October 2023, 9 of which were zero-day vulnerabilities. Actively exploited vulnerabilities that attracted the highest attention from security researchers were either observed being mass-exploited by threat actors in multiple successful cyberattack campaigns or affected the universally used HTTP/2 protocols and the GNU C Library (glibc) and had broad implications across many vendors, requiring numerous vendor-specific fixes.

First, security researchers are observing successful, ongoing mass exploitation of “Citrix Bleed” or CVE-2023-4966, a zero-day vulnerability affecting Citrix NetScaler ADC and NetScaler Gateway devices. Exploitation of CVE-2023-4966, first observed in late August 2023, is enabling various threat actors’ stealthy, persistent access to enterprise environments for ransomware deployment and more. Citrix released patches for CVE-2023-4966 on October 10, 2023. Second, a zero-day vulnerability (CVE-2023-44487) affecting the HTTP/2 protocol was exploited to enable unprecedentedly large-scale Layer 7 distributed denial-of-service (DDoS) attacks, dubbed Rapid Reset attacks, on Google, Amazon Web Services (AWS), and Cloudflare. All web applications, services, and APIs that communicate via the HTTP/2 protocol could be vulnerable to the DDoS attack if vendor-specific patches are not applied. Finally, Qualys discovered a buffer overflow vulnerability (CVE-2023-4911) called “Looney Tunables” within the GNU C Library (glibc) that, if exploited, can allow threat actors full root privileges on systems running default installations of specific Linux distributions. glibc is an important component in Linux kernel-based systems, and exploitation of this vulnerability could allow a threat actor a very high level of control in a Linux-based system.

Exploitation of such vendor-agnostic vulnerabilities that can enable significant effects and system access may appeal to threat actors, given that they can be used to target various entities across all industries. Additionally, since implementations of HTTP/2 protocol and glibc are inconsistent and vary from vendor to vendor, threat actors can leverage enterprises’ potential confusion around whether a patch exists and how and where to apply a patch for such vulnerabilities.

Other vulnerabilities were not vendor-agnostic or exploited en masse but affected a large number of organizations given the wide user bases of the products they affected:

- On October 13, 2023, Wordfence reported that threat actors were actively exploiting CVE-2023-5360, a vulnerability in a WordPress plugin used on over 200,000 websites.
- F5 warned BIG-IP administrators that sophisticated threat actors were exploiting 2 recently patched vulnerabilities in BIG-IP, CVE-2023-46747 and CVE-2023-46748, to enable stealthy cyberattacks. F5 BIG-IP is a suite of network security applications that has been widely adopted by large enterprises and government organizations.
- Microsoft announced on October 10, 2023, that it observed exploitation of the patched critical privilege escalation vulnerability in Atlassian Confluence known as CVE-2023-22515. If exploited, CVE-2023-22515 enables threat actors to create administrator accounts and gain root access, allowing them to compromise Confluence systems remotely and without user interaction and opening a pathway for data breaches and data exposure.
- Microsoft patched 2 zero-day vulnerabilities in October 2023, CVE-2023-41763 (affecting Microsoft Skype for Business Server) and CVE-2023-36563 (affecting Microsoft Windows 10, 11, Server). Neither was tied to a specific threat campaign or victim, but both were confirmed to have been exploited in the wild prior to and after patching.

Security Researchers Observe Mass Exploitation of "Citrix Bleed" CVE-2023-4966 Affecting NetScaler ADC and NetScaler Gateway Devices

Citrix released patches for CVE-2023-4966, a zero-day vulnerability affecting NetScaler ADC and NetScaler Gateway devices, on October 10, 2023. Exploitation of CVE-2023-4966 was first observed in late August 2023, is ongoing, and has enabled various threat actors' stealthy, persistent access to enterprise environments. CVE-2023-4966 is being exploited by multiple threat actors to take over authenticated sessions and circumvent credential verification measures like multifactor authentication. Hijacking of authenticated sessions allows for threat actors to acquire additional login credentials and has enabled post-exploitation activities like conducting network reconnaissance, moving laterally within networks via remote desktop protocol (RDP), and establishing stealthy persistence in target environments. Notably, these hijacked sessions might remain active even after the patch is applied, so organizations might successfully apply a patch while threat actors persist in an already-infected environment.

Assetnote published proof-of-concept (PoC) exploit code for CVE-2023-4966 on October 25, 2023. Security researcher Kevin Beaumont announced on October 28, 2023, that on that day alone, 20,000 Citrix servers were observed being attacked, resulting in the successful theft of session tokens; some of the threat activity involved the deployment of ransomware. Between October 17 and November 5, 2023, Greynoise observed over 200 distinct IP addresses attempting to exploit CVE-2023-4966, and on October 31, 2023, Mandiant warned that threat actors were continuing to exploit CVE-2023-4966 in 4 ongoing threat campaigns that have so far targeted government, technical, and legal organizations operating in the US, Europe, Africa, and Asia.

As of November 5, 2023, ShadowServer observed that nearly 4,300 servers remained exposed to the internet and vulnerable to the exploitation of CVE-2023-4966. Given the successful exploitation of this vulnerability prior to its disclosure, the mass exploitation of this vulnerability after its disclosure and PoC code was published, the public discoverability of vulnerable Citrix servers, and its continued utility in ongoing, sophisticated cybercrime campaigns, CVE-2023-4966 should be prioritized for patching immediately. As threat actors can persist stealthily in already-patched environments using already-stolen session tokens, Mandiant published some additional remediations for defenders to consider, as well as ways to detect evidence of an environment that is already infected.

Exploitation of HTTP/2 Vulnerability Enables Unprecedently Large-Scale DDoS Attacks

A zero-day vulnerability (CVE-2023-44487) affecting the HTTP/2 protocol was exploited to enable unprecedentedly large-scale Layer 7 distributed denial-of-service (DDoS) attacks, according to separate but coordinated blog posts published by Google, Amazon Web Services (AWS), and Cloudflare on October 10, 2023. Security researchers named the novel DDoS attack Rapid Reset. The attacks began in August 2023 and were ongoing in October 2023. CVE-2023-44487 is a DoS vulnerability affecting the HTTP/2 protocol that exists due to HTTP/2's improper handling of stream cancellation. HTTP/2 request cancellation capability can be abused to continuously send and cancel an unbounded number of streams from a botnet, leading to a DDoS state.

Google noted that Rapid Reset attacks were considerably larger in scale than its previously reported Layer 7 attacks. Google responded to Rapid Reset attacks that reached a record-breaking 398 million requests per second (rps). For comparison, on August 18, 2023, Google reported blocking the largest Layer 7 DDoS to date, which reached only 46 million rps. Cloudflare mitigated Rapid Reset attacks that reached 201 million rps, and Amazon reported mitigating attacks that reached 155 million rps. Cloudflare noted that the largest DDoS attack it had previously mitigated (in February 2023) only reached 71 million rps. Cloudflare also disclosed that the requests it observed originated from a 20,000-machine botnet, noting that botnets are usually "made up of hundreds of thousands or millions of machines". Cloudflare did not provide any additional information about the make or origins of the 20,000 machines.

The attacks on Google, AWS, and Cloudflare were swiftly identified and mitigated with existing DDoS protections, including those implemented in Layer 7 load balancers. Currently, CVE-2023-44487 can be fully remediated for web applications enabled by AWS Cloudfront, Cloudflare, Google Cloud, and Microsoft Azure. However, since the HTTP/2 protocol is used for approximately 40% of websites globally, the vulnerability and the DDoS attack vector have broader implications for other vendors providing web services. Patches for CVE-2023-44487 are currently vendor-specific and should be applied immediately as they become available. An aggregated list of vendor-specific advisories and mitigation suggestions can be found here. Aside from those detailed above, vendor-specific patches for CVE-2023-44487 are now available for the following vendors' products: Akka, Apache, Eclipse, F5, Facebook, Golang, Istio, Jenkins, Red Hat, Traefik Labs, Varnish Cache, and gRPC. We note Red Hat also released patches for the Looney Tunables vulnerability, detailed below. Apache and F5 implemented patches for high-risk vulnerabilities that directly affected their products this month, detailed further below.

Linux Vulnerability Tracked as CVE-2023-4911 Grants Root Access on Major Distributions

On October 3, 2023, Qualys reported that it had discovered a buffer overflow vulnerability it called "Looney Tunables," tracked as CVE-2023-4911, within the GNU C Library (glibc). glibc is an important component in Linux kernel-based systems, providing functionality for program execution, including system calls such as file operations, memory allocation, printing, and other core functions. If exploited, CVE-2023-4911 can allow threat actors full root privileges on systems running default installations of specific Linux distributions, such as Debian 12 and 13, Ubuntu 22.04 and 23.04, and Fedora 37 and 38. Dark Reading reported, "Linux root takeovers can be highly dangerous because they provide attackers with the highest level of control over a Linux-based system, and root access facilitates privilege escalation across the network, which can compromise additional systems, thus expanding the scope of the attack".

On October 9, 2023, proof-of-concept (PoC) exploit code was made publicly available for CVE-2023-4911, and on November 3, 2023, Aqua reported that it was observing Kinsing attempting to exploit CVE-2023-4911 as part of an experimental campaign aimed at compromising cloud environments.

Given its recent exploitation, defenders are urged to prioritize patching this vulnerability. Vendor-specific patches for this vulnerability have so far been applied to Fedora, GNU glibc on x64, Red Hat Enterprise Linux, and Red Hat Virtualization.

WordPress Reports Active Exploitation of WordPress Plugin Vulnerability, CVE-2023-5360

On October 13, 2023, Wordfence reported that threat actors were actively exploiting CVE-2023-5360, a vulnerability affecting Royal Elementor Addons and Templates, a WordPress plugin used on over 200,000 websites. The vulnerability “makes it possible for unauthenticated attackers to upload arbitrary files to vulnerable sites” and “can be leveraged to upload a malicious PHP file that will make remote code execution on the server possible”. Wordfence reported blocking 46,169 CVE-2023-5360 attacks and noted that the attacks were first observed on August 30, 2023. WordPress urged users to update to the latest patched version of the plugin, 1.3.79.

F5 Warns Sophisticated Threat Actors Exploiting BIG-IP Vulnerabilities to Enable Stealthy Cyberattacks

On October 26, 2023, F5 warned BIG-IP administrators that sophisticated threat actors were exploiting 2 recently patched vulnerabilities in BIG-IP, CVE-2023-46747 and CVE-2023-46748, “to erase signs of their access and achieve stealthy code execution”. F5 collected its findings via investigations of successfully compromised BIG-IP devices. F5 BIG-IP is a collection of products and services “offering load balancing, security, and performance management for networked applications that has been widely adopted by large enterprises and government organizations”. F5 urged users to apply patches to CVE-2023-46747 and CVE-2023-46748 immediately.

Microsoft Warns Storm-0062 Nation-State Hackers Exploiting Critical Atlassian Confluence Vulnerability

Microsoft observed exploitation of the patched critical privilege escalation vulnerability in Atlassian Confluence known as CVE-2023-22515, the company announced on October 10, 2023. Microsoft observed exploitation activity by the state-sponsored group known as Storm-0062 (DarkShadow or Oro0lxy) beginning on September 14, 2023.

On October 4, 2023, Atlassian disclosed and patched the privilege escalation vulnerability, which affects its Confluence Data Center and Confluence Server versions 8.0.0 through 8.5.1. If exploited, it enables threat actors to create administrator accounts and gain root access, allowing them to compromise Confluence systems remotely and without user interaction (exploitation of the vulnerability is further discussed in the Recorded Future Data section below). This compromise opens a pathway for data breaches and data exposure by threat actors.

Based on the window between Microsoft exploitation observation and Atlassian’s patch release, threat actors exploited the vulnerability as a zero-day for 3 weeks: from September 14 to October 4, 2023. Now that a patch is available, Atlassian has encouraged users, especially those who operate within sectors that Storm-0062 has previously targeted, to upgrade to patched versions (8.3.3, 8.4.3, 8.5.2, or later) and, when immediate upgrading is infeasible, to either disable or isolate their systems from the internet to guard against possible exploitation.

HelloKitty Ransomware Gang Exploits CVE-2023-46604 Vulnerability in Apache ActiveMQ

Rapid7 reported on November 1, 2023, that the HelloKitty Ransomware Gang has been exploiting a remote code execution (RCE) vulnerability in Apache ActiveMQ, tracked as CVE-2023-46604, with the intent of deploying HelloKitty ransomware in customer environments. If exploited, the vulnerability allows threat actors to execute commands using the OpenWire protocol's serialized class types. Despite the release of the security update for affected ActiveMQ versions (5.15.16, 5.16.7, 5.17.6, and 5.18.3) on October 25, 2023, approximately 3,329 internet-exposed servers remained vulnerable.

Once the exploitation was successful, threat actors attempted to load MSI files named “M2.png” and “M4.png” using the Windows Installer. These files contained a .NET executable that loaded a base64-encoded .NET DLL named EncDLL. Upon execution, EncDLL targeted specific processes, encrypted files, appended a ".locked" extension, and dropped a ransom note directing communications to the email address *service@hellokittycat[.]online* (Intelligence Card). A proof-of-concept (POC) exploit for CVE-2023-46604 was released via GitHub.

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-2023-44487	99	Any product that uses the HTTP/2 protocol	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly. Fixes are vendor-specific.	N/A	Yes
2	CVE-2023-41763	99	Microsoft Skype for Business Server	Skype for Business Elevation of Privilege Vulnerability	N/A	Yes
3	CVE-2023-36563	99	Microsoft Windows 10, 11, Server	Microsoft WordPad Information Disclosure Vulnerability	N/A	Yes
4	CVE-2023-4966	99	Citrix NetScaler ADC and NetScaler Gateway	A sensitive information disclosure vulnerability that allows an attacker to read large amounts of memory after the end of a buffer	Unspecified Ransomware	Yes
5	CVE-2023-5360	99	WordPress Royal Elementor Addons 1.3.78	The Royal Elementor Addons and Templates WordPress plugin before 1.3.79 does not properly validate uploaded files, which could allow unauthenticated users to upload arbitrary files, such as PHP and achieve RCE.	N/A	Yes
6	CVE-2023-46747	99	F5 BIG-IP	Undisclosed requests may bypass configuration utility authentication, allowing attackers with network access to the BIG-IP system through the management port and/or self-IP addresses to execute arbitrary system commands.	N/A	Yes

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/ Component	Malware	Zero-Day
7	CVE-2023-46748	99	F5 BIG-IP	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility that may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self-IP addresses to execute arbitrary system commands.	N/A	Yes
8	CVE-2023-46604	99	Apache ActiveMQ	Apache ActiveMQ is vulnerable to Remote Code Execution. The vulnerability may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath.	HelloKitty Ransomware	No
9	CVE-2023-36731	91	Microsoft Windows 10, 11, Server	Win32k Elevation of Privilege Vulnerability	N/A	No
10	CVE-2023-22515	89	Atlassian Confluence Data Center, Confluence Server	Atlassian has been made aware of an issue reported by a handful of customers where external attackers may have exploited a previously unknown vulnerability in publicly accessible Confluence Data Center and Server instances to create unauthorized Confluence administrator accounts and access Confluence instances.	N/A	Yes
11	CVE-2023-42824	89	Apple iPad OS, iPhone OS	Apple iOS and iPadOS Kernel Privilege Escalation Vulnerability	N/A	Yes
12	CVE-2023-4911 (Looney Tunables)	79	Fedora GNU glibc on x64 Red Hat Enterprise Linux Red Hat Virtualization	A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.	N/A	No
13	CVE-2023-43641	79	Debian Linux Fedora Lipnitsk Libcue	A vulnerability in libcue, which can lead to code execution by downloading a file on GNOME	N/A	No
14	CVE-2023-38545	79	Cisco Adaptive	A heap-based buffer overflow flaw that affects	N/A	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/ Component	Malware	Zero-Day
			Security Appliance ASA Software Cisco Crosswork Network Change Automation Cisco Secure Network Analytics Haxx libcurl 7.69.0	both libcurl and the curl command-line tool itself		
15	CVE-2023-5044	76	Kubernetes Ingress-nginx	Code injection via nginx.ingress.kubernetes.io/ permanent-redirect annotation	N/A	No
16	CVE-2023-35803	75	Extremenetworks IQ ENGINE	CVE-2023-35803 is a critical unauthenticated Remote Code Execution (RCE) vulnerability that affects Extreme Networks/Aerohive Wireless Access Points	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.