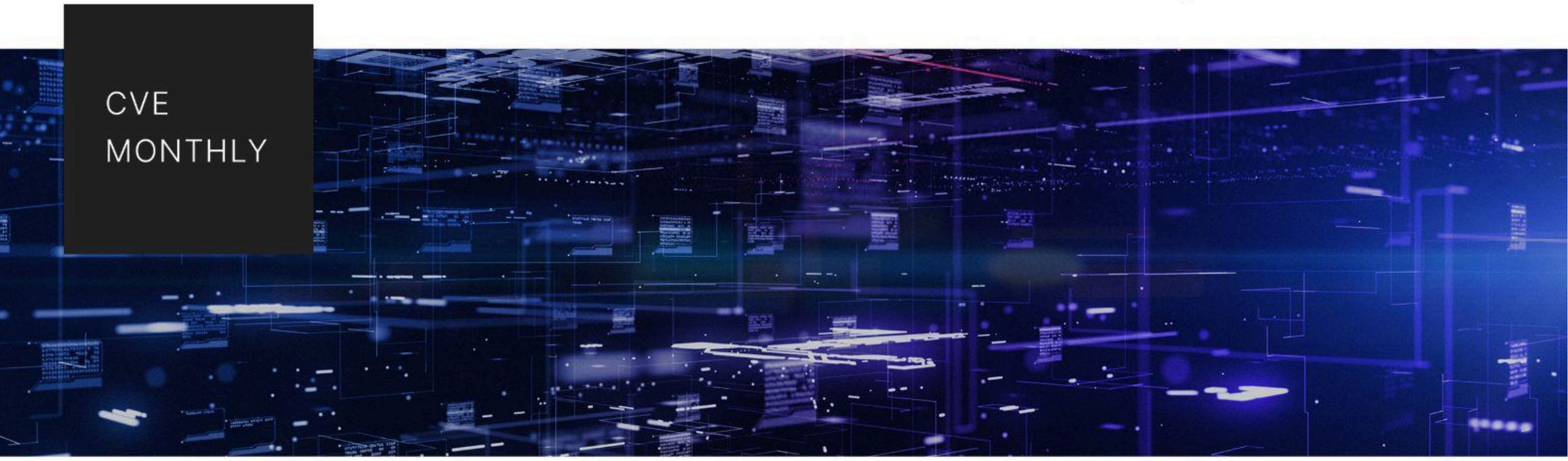
CVE
MONTHLY



Recorded Future CVE Monthly January 2024

This report primarily analyzes the top vulnerabilities disclosed across eight major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from January 1 to 31, 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 January 2024, eight newly disclosed, actively exploited vulnerabilities affected Atlassian Confluence, Jenkins automation software, Citrix NetScaler, various Apple products, Google Chrome, and Ivanti Connect.
- Atlassian Confluence, Jenkins automation software, Fortra's GoAnywhere managed file transfer (MFT) service, and Ivanti Connect Secure VPN devices saw the active exploitation of severe vulnerabilities that can enable an unauthenticated attacker to access sensitive data or carry out remote code execution (RCE) in restricted enterprise systems.
- A critical vulnerability (CVE-2024-0204) in GoAnywhere can enable unauthenticated attackers administrative access to the MFT service; exploitation of a similar vulnerability (CVE-2023-0669) enabled ransomware attacks on approximately 130 high-profile enterprises in early 2023.
- 27 of the approximately 2,500 vulnerabilities disclosed in January 2024 were high-risk, according to Recorded Future data.

CVE Monthly Prominent Vulnerability Disclosures

In January 2024, we identified 27 high-risk vulnerabilities, eight of which are known to be exploited in the wild and should be prioritized for remediation.

The most prominent vulnerability trend in January 2024 was the disclosure of several actively exploited severe vulnerabilities in enterprise software that can enable unauthenticated threat actors to access sensitive data or carry out remote code execution (RCE) in restricted enterprise systems. These very high-risk vulnerabilities, bearing CVSSv3.1 scores of 9 and above, affected Atlassian Confluence Data Center and Server, Jenkins 2.441 and earlier, LTS 2.426.2 and earlier, Fortra's GoAnywhere managed file transfer (MFT) service, and Ivanti Connect Secure (ICS) VPN devices. In most cases, these services and product offerings were affected by singular severe vulnerabilities; however, in the case of Ivanti Connect Secure (ICS) VPN devices, threat actors chained the exploitation of 2 vulnerabilities together to enable unauthenticated RCE. All these vulnerabilities are confirmed to have been actively exploited in the wild. While details in open sources on specific attacks enabled by exploitation of these vulnerabilities are sparse, they remain critical vulnerabilities to remediate immediately, for reasons outlined below.

Many instances of the services affected by these vulnerabilities are publicly discoverable via Internet scan, which, combined with the ease of exploitation of these vulnerabilities, the availability of proof-of-concept (PoC) exploit code, and confirmed active exploitation of most of these vulnerabilities, makes them critical to prioritize for immediate remediation.

CVE-2024-0204 is a particularly important vulnerability to remediate, given that another GoAnywhere vulnerability, CVE-2023-0669, was mass-exploited by CL0P ransomware group (CL0P) to enable a number of high-profile ransomware attacks on approximately 130 enterprises, including Saks Fifth Avenue and Hitachi Energy in early 2023. CVE-2023-0669 allows for RCE, but requires access to the administrative console of the GoAnywhere MFT, making CVE-2024-0204 an easier vulnerability to exploit. CVE-2024-0204 is a critical authentication bypass vulnerability that can enable unauthenticated attackers to gain administrative access by creating a new user via the

GoAnywhere administrator portal. Details of all these vulnerabilities and other vulnerabilities with 99+ risk scores, according to Recorded Future data, are provided below.

Atlassian Addresses Critical Remote Code Execution Vulnerability CVE-2023-22527 in Confluence Data Center and Server

Atlassian addressed a critical vulnerability, tracked as CVE-2023-22527 (CVSSv3.1 score: 9.8), in the Confluence Data Center and Server on January 16, 2024. The Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2023-22527 to its Known Exploited Vulnerabilities (KEV) catalog on January 31, 2024. Successful exploitation of CVE-2023-22527 enables threat actors to execute arbitrary code on systems running Confluence Data Center and Server versions 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, and 8.5.0-8.5.3. This allows unauthorized access to sensitive data, disruption of system operations, and further compromise within the network.

Critical Vulnerability (CVE-2024-23897) in Jenkins Automation Software Makes Servers Vulnerable to Remote Code Execution

On January 24, 2024, Jenkins disclosed CVE-2024-23897 (CVSSv3.1 score: 9.8), a critical arbitrary file read vulnerability in its open-source continuous integration/continuous delivery and deployment (CI/CD) automation software. CVE-2024-23897 can enable an unauthenticated threat actor to read files on the Jenkins controller file system and potentially carry out remote code execution (RCE). The flaw exists in Jenkins's built-in command-line interface (CLI), which enables access to Jenkins from a script or shell environment. According to Horizon.ai analysis, Jenkins has "hundreds of thousands" of public-facing endpoints, and Shadowserver data found approximately 45,000 servers are vulnerable to CVE-2024-23897. The Cyber Security Agency (CSA) of Singapore reported that as of January 30, 2024, the vulnerability was being actively exploited.

According to Jenkins, the flaw can be used to read binary files containing cryptographic keys and potentially enable the following types of attacks:

- RCE via Resource Root URLs
- RCE via "Remember me" cookie
- RCE via stored cross-site scripting (XSS) attacks through build logs
- RCE via Cross-Site Request Forgery (CSRF) protection bypass
- Decrypt secrets stored in Jenkins
- Delete any item in Jenkins
- Download a Java heap dump

Since its disclosure, several proof-of-concept (PoC) exploit codes for CVE-2024-23897 have been published to GitHub, increasing the chances of this vulnerability being exploited in the wild. CVE-2024-23897 is remediated with Jenkins's release of Jenkins 2.442 and Jenkins LTS 2.426.3. Enterprises unable to update to Jenkins 2.442 and LTS 2.426.3 immediately are advised to disable access to Jenkins's CLI feature until an update can be applied. Jenkins provided instructions for this workaround via GitHub.

Threat actors have previously exploited vulnerabilities in Jenkins products because of their widespread usage (about 44% of the CI/CD market in 2023) as well as the sensitive software information handled by CI/CD products. Threat actors with access to this type of sensitive information have the capacity to disrupt the software pipeline, exposing downstream users to risks like poisoned code and compromised products.

CVE-2024-0204 (Fortra GoAnywhere MFT) Can Enable Unauthenticated Attacker Administrative Access

On January 22, 2024, Fortra disclosed CVE-2024-0204 (CVSSv3.1 score: 9.0), an authentication bypass vulnerability affecting Fortra's GoAnywhere managed file transfer (MFT) service versions prior to 7.4.1. CVE-2024-0204 is a critical authentication bypass vulnerability that can enable unauthenticated attackers to gain administrative access by creating a new user via the GoAnywhere administrator portal.

CVE-2024-0204 was previously disclosed to Fortra customers via internal notifications and patched with the December 7, 2023, release of GoAnywhere version 7.4.1. January 22, 2024, marked the first public disclosure of CVE-2024-0204. On January 23, 2024, Security Boulevard published proof-of-concept (PoC) exploit code for the vulnerability.

Widespread Exploitation of CVE-2023-46805 and CVE-2024-21887 Vulnerabilities in Ivanti Connect Secure VPN devices

On January 10, 2024, Volexity reported widespread exploitation of two zero-day vulnerabilities in Ivanti Connect Secure (ICS) VPN devices, tracked as CVE-2023-46805 and CVE-2024-21887. Threat actors chain exploitation of both vulnerabilities together to enable unauthenticated RCE. This exploitation was carried out by multiple threat actors, including a Chinese state-sponsored threat actor tracked as "UTA0178". These vulnerabilities are as follows:

- CVE-2023-46805: An authentication bypass vulnerability within the web element of the gateways, allowing threat actors to access restricted resources by evading security validations.

- CVE-2024-21887: A code injection vulnerability that, if exploited, enables threat actors to execute arbitrary commands within the affected appliances through specially crafted requests.

The impact of this exploitation spans a broad range of sectors globally, including government, military, telecommunications, defense, technology, finance, and aerospace industries. This widespread reach highlights the severity of the threat.

The combination of CVE-2023-46805 and CVE-2024-21887 enables unauthenticated RCE across all supported ICS VPN versions. Volexity's observations reveal that around 1,700 devices have been compromised using a modified GIFTEDVISITOR webshell. Mandiant identified five custom malware strains used by UTA0178, including ZIPLINE, LIGHTWIRE, THINSPOOL, WIREFIRE, and WARPWIRE, which play crucial roles in persistence, evasion, command execution, and credential theft.

On February 1, 2023, Ivanti released patches for CVE-2023-46805 and CVE-2024-21887.

Citrix Addresses CVE-2023-6548 and CVE-2023-6549 Vulnerabilities on Its Netscaler ADC and Gateway Appliances

On January 17, 2024, Citrix patched two actively exploited critical vulnerabilities, tracked as CVE-2023-6548 and CVE-2023-6549, in its Citrix Netscaler Application Delivery Controller (ADC) and Citrix Netscaler Access Gateway appliances. The same day, CISA added both vulnerabilities to its KEV catalog. Citrix noted that CVE-2023-6548 only affected customer-managed NetScaler appliances, ensuring the security of Citrix-managed cloud services.

Citrix urges customers to promptly patch vulnerable appliances and separate network traffic to the appliance's management interface. For those unable to patch immediately, it's crucial to block network traffic to affected appliances and limit their internet exposure to mitigate exploitation risks.

At the time of writing, approximately 1,400 Netscaler management interfaces were publicly accessible online, according to Shadowserver.

The affected Netscaler product versions include 14.1-12.35, 13.1-51.15, 13.0-92.21 for NetScaler ADC and NetScaler Gateway, and 13.1-37.176, 12.1-55.302, and 12.1-55.302 for specific NetScaler ADC configurations. Details of the vulnerabilities are as follows:

- CVE-2023-6548: A remote code execution vulnerability that can only be exploited by threat actors who are logged into low-privilege accounts with access to the Netscaler management interface, as well as NetScaler IP (NSIP), Cluster IP (CLIP), and Subnet IP (SNIP).

- CVE-2023-6549: An unauthenticated denial-of-service (DoS) vulnerability that requires an appliance to be configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or an AAA virtual server to be exposed to DoS attacks.

Apple Addresses CVE-2024-23222 Vulnerability on Its iPhones, Macs, and Apple TVs
On January 22, 2024, Apple patched a WebKit confusion vulnerability, tracked as CVE-2024-23222, in its iPhone, Mac, and Apple TV devices. If exploited, CVE-2024-23222 could allow threat actors to execute arbitrary malicious code on affected devices by luring victims into visiting a malicious web page. The affected Apple product versions include iOS 16.7.5, iPadOS 16.7.5, macOS Monterey 12.7.3, and tvOS 17.3.

Apple acknowledged the exploitation but did not disclose specific details about the threat actors or the attack vectors. Apple also recommended that users promptly install the provided security updates.

Google Chrome Update Addresses Actively Exploited Zero-Day CVE-2024-0519 and Two Vulnerabilities
Google released an update for the Chrome browser to address an actively exploited vulnerability tracked as CVE-2024-0519, along with two other vulnerabilities within the V8 JavaScript engine. The update, issued on January 16, 2024, is for Chrome versions 120.0.6099.224/225 on Windows, 120.0.6099.234 on Mac, and 120.0.6099.224 on Linux. CVE-2024-0519 involves a heap buffer overflow vulnerability, enabling threat actors to execute arbitrary code on compromised systems. Google has not disclosed additional information about exploitation activity for CVE-2024-0519. This decision is part of a strategy to prevent further exploitation and to provide users time to apply the necessary updates to secure their systems against these vulnerabilities.

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-2023-22527	99	Atlassian Confluence Data Center and Server versions 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, and 8.5.0-8.5.3	A template injection vulnerability on older versions of Confluence Data Center and Server allows an unauthenticated attacker to achieve RCE on an affected instance. Customers using an affected version must take immediate action.	Yes
2	CVE-2024-23897	99	Jenkins 2.441 and earlier, LTS 2.426.2 and earlier	Jenkins 2.441 and earlier, and LTS 2.426.2 and earlier, does not disable a feature of its CLI command parser that replaces an "@" character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.	Yes
3	CVE-2024-0204	99	Fortra's GoAnywhere MFT prior to 7.4.1	Authentication bypass in Fortra's GoAnywhere MFT prior to 7.4.1 allows an unauthorized user to create an admin user via the administration portal.	Yes
4	CVE-2024-21887	99	Ivanti Connect Secure, Ivanti Policy Secure	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. Chained with exploitation of CVE-2023-46805 to enable unauthenticated RCE.	Yes
5	CVE-2023-6549	99	Citrix NetScaler ADC and NetScaler Gateway: 14.1-12.35, 13.1-51.15, 13.0-92.21; Specific NetScaler ADC configurations: 13.1-37.176, 12.1-55.302, and 12.1-55.302	Improper restriction of operations within the bounds of a memory buffer in NetScaler ADC and NetScaler Gateway allows unauthenticated denial-of-service.	Yes
6	CVE-2023-6548	99	Citrix NetScaler ADC and NetScaler Gateway: 14.1-12.35, 13.1-51.15, 13.0-92.21; Specific NetScaler ADC configurations: 13.1-37.176, 12.1-55.302, and 12.1-55.302	Improper control of generation of code ("Code Injection") in NetScaler ADC and NetScaler Gateway allows an attacker with access to NSIP, CLIP, or SNIP with management interface to perform authenticated (low-privileged) remote code execution on Management Interface.	Yes
7	CVE-2024-23222	99	Apple iOS 16.7.5, iPadOS 16.7.5, macOS Monterey 12.7.3, and tvOS 17.3	A type confusion issue was addressed with improved checks. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited. This issue is fixed in tvOS 17.3, iOS 17.3,	Yes

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
				and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, and macOS Monterey 12.7.3.	
8	CVE-2024-0519	99	Google Chrome prior to 120.0.6099.224	Out-of-bounds memory access in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High.)	Yes
9	CVE-2023-21674	79	Microsoft Windows 10, 11, Server	Windows Advanced Local Procedure Call (ALPC) elevation-of-privilege vulnerability.	No
10	CVE-2023-5356	79	GitLab CE/EE all versions from 8.13 before 16.5.6, versions from 16.6 before 16.6.4, versions from 16.7 before 16.7.2	Incorrect authorization checks in GitLab CE/EE from all versions starting from 8.13 before 16.5.6, all versions starting from 16.6 before 16.6.4, all versions starting from 16.7 before 16.7.2, allows a user to abuse slack/mattermost integrations to execute slash commands as another user.	No
11	CVE-2024-21591	79	Junos OS, various versions	An out-of-bounds write vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to cause a denial-of-service (DoS), or remote code execution (RCE) and obtain root privileges on the device. This issue is caused by the use of an insecure function allowing an attacker to overwrite arbitrary memory.	No
12	CVE-2022-1609	79	Weblizar School Management Pro Edition for WordPress, various versions	The School Management WordPress plugin before 9.9.7 contains an obfuscated backdoor injected in its license checking code that registers a REST API handler, allowing an unauthenticated attacker to execute arbitrary PHP code on the site.	No
13	CVE-2024-20656	79	Microsoft Visual Studio, various versions	Visual Studio elevation-of-privilege vulnerability.	No
14	CVE-2023-40547	79	Red Hat Enterprise Linux and Red Hat Shim, various versions	A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise.	No
15	CVE-2023-50643	79	Evernote 10.68.2 for macOS	An issue in Evernote for MacOS v.10.68.2 allows a remote attacker to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments components.	No
16	CVE-2024-20253	79	Cisco Adaptive Security Appliance (ASA) Software, Cisco Packaged Contact Center Enterprise, Cisco Unified Communications Manager, Cisco Unity	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
			Connection Software, Cisco Virtualized Voice Browser	could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device.	
17	CVE-2024-20272	79	Cisco Unity Connection Software	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system. This vulnerability is due to a lack of authentication in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by uploading arbitrary files to an affected system. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root.	No
18	CVE-2023-6000	79	Sygnoos Popup Builder for WordPress	The Popup Builder WordPress plugin before 4.2.3 does not prevent simple visitors from updating existing popups and injecting raw JavaScript in them, which could lead to Stored XSS attacks.	No
19	CVE-2024-0200	79	GitHub Enterprise Server	An unsafe reflection vulnerability was identified in GitHub Enterprise Server that could lead to reflection injection. This vulnerability could lead to the execution of user-controlled methods and remote code execution. To exploit this bug, an actor would need to be logged into an account on the GHES instance with the organization owner role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.13, 3.9.8, 3.10.5, and 3.11.3. This vulnerability was reported via the GitHub Bug Bounty program.	No
20	CVE-2024-0517	79	Google Chrome prior to 120.0.6099.224	Out-of-bounds write in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High.)	No
21	CVE-2024-20674	78	Microsoft Windows 10, 11, Server	Windows Kerberos Security Feature Bypass Vulnerability.	No
22	CVE-2023-41474	77	Ivanti Avalanche 6.3.4.153 Premise Edition	Directory Traversal vulnerability in Ivanti Avalanche 6.3.4.153 allows a remote authenticated attacker to obtain sensitive information via the javax.faces.resource component.	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
23	CVE-2023-6875	76	WPExperts Post SMTP for WordPress, various versions	The POST SMTP Mailer – Email log, Delivery Failure Notifications and Best Mail SMTP for WordPress plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a type juggling issue on the connect-app REST endpoint in all versions up to and including 2.8.7. This makes it possible for unauthenticated attackers to reset the API key used to authenticate to the mailer and view logs, including password reset emails, allowing site takeover.	No
24	CVE-2023-39336	75	Ivanti Endpoint Manager 2016, 2017, 2018, 2019, 2020, 2021, 2022	An unspecified SQL Injection vulnerability in Ivanti Endpoint Manager released prior to 2022 SU 5 allows an attacker with access to the internal network to execute arbitrary SQL queries and retrieve output without the need for authentication. Under specific circumstances, this may also lead to RCE on the core server.	No
25	CVE-2023-50919	75	GL.iNET GL-A1300 Firmware	An issue was discovered on GL.iNet devices before version 4.5.0. There is an NGINX authentication bypass via Lua string pattern matching. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	No
26	CVE-2024-23898	75	Jenkins 2.441 and earlier, LTS 2.426.2 and earlier	Jenkins 2.217 through 2.441 (both inclusive), and LTS 2.222.1 through 2.426.2 (both inclusive), do not perform origin validation of requests made through the CLI WebSocket endpoint, resulting in a cross-site WebSocket hijacking (CSWSH) vulnerability, allowing attackers to execute CLI commands on the Jenkins controller.	No
27	CVE-2024-0402	75	GitLab Community Edition, Enterprise Edition	An issue has been discovered in GitLab CE/EE affecting all versions from 16.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1, which allows an authenticated user to write files to arbitrary locations on the GitLab server while creating a workspace.	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.