



Threat Level

 Red

 CISA:AA23-215A

HiveForce Labs

# THREAT ADVISORY

 VULNERABILITY REPORT

## 2022 Most Consistently Exploited Vulnerabilities

Date of Publication

August 4 , 2023

Admiralty Code

A1

TA Number













TA2023322

# Summary

**Affected Products:** FortiOS, FortiProxy, Microsoft Exchange Server, Zoho ManageEngine, Atlassian Confluence Server and Data Center, Apache Log4j2, VMware Workspace, and F5 Networks BIG-IP

**Impact:** This advisory presents comprehensive information regarding the Common Vulnerabilities and Exposures (CVEs) consistently and frequently targeted by malicious cyber adversaries throughout the year 2022 across multiple vendors, encompassing Fortinet, Microsoft, Zoho ManageEngine, Atlassian, Apache, VMware, and F5 BIG-IP. Notably, among these, four Zero-day vulnerabilities were also exploited by adversaries.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2018-13379	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	Fortinet FortiOS			
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability (PROXYSHELL)	Microsoft Exchange Server			
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability (PROXYSHELL)	Microsoft Exchange Server			
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability (PROXYSHELL)	Microsoft Exchange Server			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability	Zoho ManageEngine			
CVE-2021-26084	Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability	Atlassian Confluence Server and Data Center			
CVE-2021-44228	Apache Log4j2 Remote Code Execution Vulnerability (LOG4J)	Apache Log4j2			
CVE-2022-22954	VMware Workspace ONE Access and Identity Manager Server-Side Template Injection Vulnerability	VMware Workspace ONE Access and Identity Manager			
CVE-2022-22960	VMware Multiple Products Privilege Escalation Vulnerability	VMware Multiple Products			
CVE-2022-1388	F5 BIG-IP Missing Authentication Vulnerability	F5 BIG-IP			
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (FOLLINA)	Microsoft Windows			
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server/Data Center			

# Vulnerability Details

## #1

In 2022, malicious cyber actors consistently and frequently exploited several CVEs across various vendors, including Fortinet, Microsoft, Zoho ManageEngine, Atlassian, Apache, VMware, and F5 BIG-IP. Notably, four Zero-day vulnerabilities were among the targets of these adversaries. Specifically, a group of unidentified Iranian attackers and the Lockbit ransomware leveraged the CVE-2018-13379 vulnerabilities to carry out their ransom operations. This flaw was exploited with significant effect.

## #2

Another critical vulnerability, CVE-2021-34473, found in Microsoft Exchange Server, became a favored tool for various threat actors. The LV ransomware-as-a-service, ChamelGang Strikes (which deployed ChamelDoH Malware), Cadet Blizzard APT (responsible for deploying WhisperGate malware), and Iranian government-sponsored actors all made use of this particular CVE to execute diverse campaigns.

## #3

CVE-2021-31207, on the other hand, was utilized by the Cadet Blizzard APT (deploying WhisperGate malware), Iranian government-sponsored actors, and ChamelGang Strikes (deploying ChamelDoH Malware). This vulnerability served a dual purpose: unauthorized access and compromising organizations, leading to the installation of cryptocurrency miners.

## #4

In the realm of Apache vulnerabilities, Log4J tracked CVE-2021-44228 was exploited by the Monti ransomware and MuddyWater to target Israeli organizations. Additionally, the Budworm espionage group took advantage of Log4j vulnerabilities to undermine the Apache Tomcat service.

## #5

Lastly, the GoldenJackal APT successfully exploited CVE-2022-30190 to deploy a range of custom malware, primarily focusing on targets in the Middle East and South Asia. Throughout 2022, these attackers demonstrated their proficiency in identifying and exploiting specific CVEs. Apart from the Top 12 vulnerabilities, there exists a multitude of other identified weaknesses that were consistently exploited by malicious cyber actors throughout 2022.

## Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2021-34473	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2013 Cumulative Update 23 15.00.1497.002	cpe:2.3:a:microsoft:exchange_server:- :*:*:*:*:*	CWE-918

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2018-13379	FortiOS: 5.6.3 - 6.0.4	cpe:2.3:o:fortinet:fortios:*.~*~*~*~*~*~*~*~*~*	CWE-22
CVE-2021-31207	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2019 Cumulative Update 9 15.02.0858.005	cpe:2.3:a:microsoft:exchange_server:-:~*~*~*~*~*~*~*~*~*	CWE-22
CVE-2021-34523	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2013 Cumulative Update 23 15.00.1497.002	cpe:2.3:a:microsoft:exchange_server:-:~*~*~*~*~*~*~*~*~*	CWE-287
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus: 6000 - 6113	cpe:2.3:a:zohocorp:manageengine_adservice_plus:-:~*~*~*~*~*~*~*~*~*	CWE-287
CVE-2021-26084	Atlassian Confluence Server: 6.0.1 - 7.12.4	cpe:2.3:a:atlassian:confluence_data_center:~*~*~*~*~*~*~*~*~*	CWE-74
CVE-2021-44228	Apache Log4j: 2.0 - 2.14.1	cpe:2.3:a:apache:log4j:-:~*~*~*~*~*~*~*~*~*	CWE-917, CWE-400, CWE-20, CWE-502
CVE-2022-22954	VMware Workspace ONE Access: 20.10.0.0 - 21.08.0.1	cpe:2.3:a:vmware:identity_manager:-:~*~*~*~*~*~*~*~*~*	CWE-94
CVE-2022-22960	VMware Workspace ONE Access: 20.10.0.0 - 21.08.0.1	cpe:2.3:a:vmware:cloud_foundation:~*~*~*~*~*~*~*~*~*~*	CWE-269
CVE-2022-1388	BIG-IP: 11.6.1 - 16.1.2.1	cpe:2.3:a:f5:big-ip_access_policy_manager:~*~*~*~*~*~*~*~*~*	CWE-306
CVE-2022-30190	Windows Server: 2008 – 2022, Windows: 7 - 11 21H2	cpe:2.3:o:microsoft:windows:-:~*~*~*~*~*~*~*~*~*	CWE-78
CVE-2022-26134	Atlassian Confluence Server: 5.0 - 7.18.0 Jira Data Center: 6.0.0 - 8.22.3	cpe:2.3:a:atlassian:confluence_data_center:~*~*~*~*~*~*~*~*~*	CWE-74

# Recommendations



**Exposure Management:** Perform a service exposure assessment to identify any vulnerable services exposed. Take immediate action to patch any identified vulnerabilities or implement complementary controls to enhance security.



**Update System:** Ensure your systems are up to date by installing the latest security updates. Follow device-specific security best practices to prevent any additional vulnerabilities from emerging. Also, validate the configurations of internet-facing devices and applications.



**Monitor:** Maintain vigilant monitoring of all security-related events in devices and applications. In case of any anomalies, promptly initiate the incident management process.



**Backup:** Confirm regular backups for all assets. Ensure backups are adequately protected, employ the 3-2-1 backup principle, and deploy specialized tools to ensure backup integrity and availability.



## Potential MITRE ATT&CK TTPs

<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0005</u></b> Defense Evasion
<b><u>TA0040</u></b> Impact	<b><u>T1203</u></b> Exploitation for Client Execution	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1068</u></b> Exploitation for Privilege Escalation
<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1588.005</u></b> Exploits	<b><u>T1040</u></b> Network Sniffing
<b><u>T1005</u></b> Data from Local System	<b><u>T1036</u></b> Masquerading	<b><u>T1574</u></b> Hijack Execution Flow	<b><u>T1211</u></b> Exploitation for Defense Evasion

## Patch Links

<https://fortiguard.com/advisory/FG-IR-18-384>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523>

<https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html>

<https://jira.atlassian.com/browse/CONFSERVER-67940>

<https://logging.apache.org/log4j/2.x/security.html>

<https://www.vmware.com/security/advisories/VMSA-2022-0011.html>

<https://support.f5.com/csp/article/K23605346>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190>

<https://jira.atlassian.com/browse/CONFSERVER-79016>

## References

[https://www.cisa.gov/sites/default/files/2023-08/aa23-215a\\_joint\\_csa\\_2022\\_top\\_routinely\\_exploited\\_vulnerabilities.pdf](https://www.cisa.gov/sites/default/files/2023-08/aa23-215a_joint_csa_2022_top_routinely_exploited_vulnerabilities.pdf)

<https://www.hivepro.com/the-8220-cryptomining-gang-massively-expands-cloud-botnets/>

<https://www.hivepro.com/unveiling-the-stealthy-operations-of-goldenjackal-apt-group/>

<https://www.hivepro.com/asylum-ambuscade-unmasking-the-hybrid-threat-group-in-cybersecurity/>

<https://www.hivepro.com/muddywater-targets-israeli-organizations-by-exploiting-unpatched-log4j-vulnerabilities/>

<https://www.hivepro.com/monti-ransomware-infiltrates-networks-via-the-well-known-log4shell/>

<https://www.hivepro.com/budworm-attackers-return-with-new-espionage-strikes-against-the-united-states/>

<https://www.hivepro.com/volt-typhoon-chinese-espionage-group-targets-u-s-government/>

<https://www.hivepro.com/unknown-iranian-attackers-leverage-vulnerabilities-to-conduct-ransom-operations/>

<https://www.hivepro.com/lockbit-ransomware-evolving-tactics-and-pervasive-impact-in-2023/>

<https://www.hivepro.com/unveiling-cadet-blizzard-apt-wiper-attacks-targeting-ukraine/>

<https://www.hivepro.com/chamelgang-strikes-again-with-chameldoh-malware-xdns-over-https/>

<https://www.hivepro.com/proxyshellminer-exploits-windows-exchange-server-vulnerabilities-for-cryptocurrency-mining/>

<https://www.hivepro.com/lv-ransomware-exploited-proxyshell-to-target-jordan/>

<https://www.hivepro.com/blackcat-ransomware-group-implements-quadruple-extortion/>

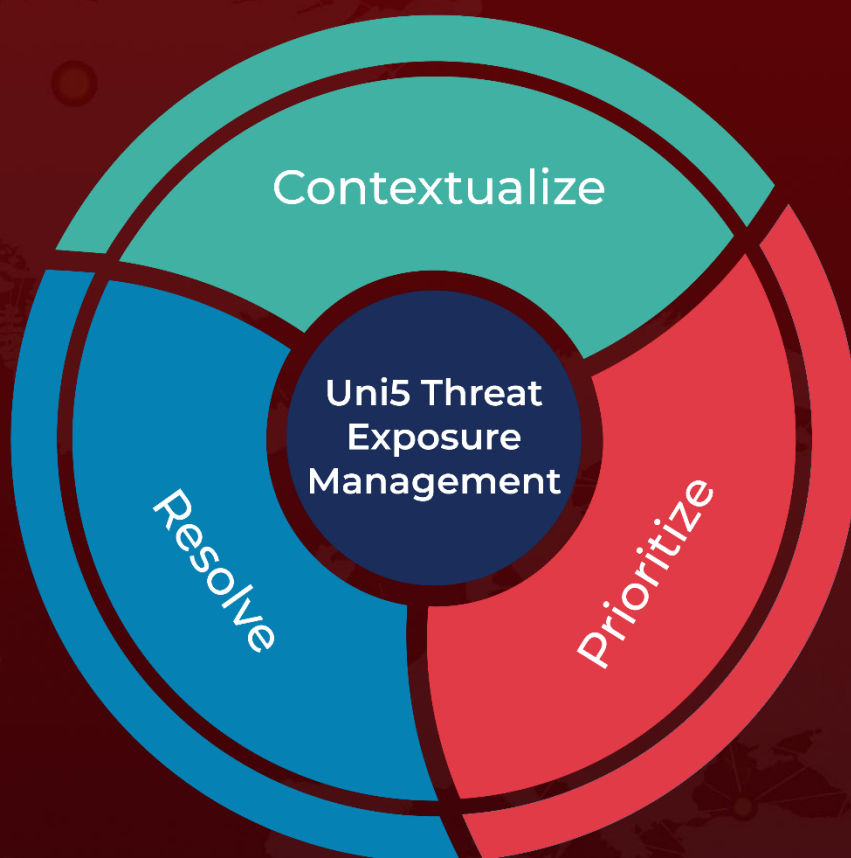
<https://www.hivepro.com/worok-cyber-espionage-gang-preys-on-high-profile-asian-businesses-and-governments/>



# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**August 4, 2023 • 8:30 AM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)