Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

Vulnerable Atlassian Confluence Servers utilized to drop Crypto Miners

Date of Publication	Admiralty Code	TA Number
September 22, 2022	A1	TA2022211

Summary

The Atlassian Confluence Server's CVE-2022-26134, an unauthenticated remote code execution (RCE) vulnerability that was recently patched, is being used by adversaries to deploy cryptocurrency mining malware.

CVEs Table

CVE	NAME	PATCH
CVE-2022-26134	Unauthenticated remote code execution vulnerability in Confluence	✓
CVE-2021-4034	A local privilege escalation vulnerability in polkit's pkexec utility (PwnKit)	✓

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0008** Lateral Movement	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**T1053** Scheduled Task/Job	**T1053.003** Cron	**TA0040** Impact
T1496 Resource Hijacking	**TA0005** Defense Evasion	**TA0007** Discovery	**T1070.004** File Deletion
T1574.007 Path Interception by PATH Environment Variable	**T1222** File and Directory Permissions Modification	**T1222.002** Linux and Mac File and Directory Permissions Modification	**T1562** Impair Defenses
T1574 Hijack Execution Flow	**T1562.004** Disable or Modify System Firewall	**T1564** Hide Artifacts	**T1564.001** Hidden Files and Directories
T1574 Hijack Execution Flow	**T1518** Software Discovery	**T1082** System Information Discovery	**T1018** Remote System Discovery
T1021 Remote Services	**T1070** Indicator Removal on Host	**T1190** Exploit Public-Facing Application	

Technical Details

#1

The infection chain began by exploiting the vulnerability by sending a specially crafted HTTP request to the target server that included an Object-Graph Navigation Language (OGNL) expression in the HTTP request Uniform Resource Identifier (URI), resulting in remote code execution (RCE).

#2

Then the ro.sh/ap.sh shell script files are executed, which perform a variety of malicious behaviors, such as deploying a curl binary file from the command and control (C2) server. The script downloads a binary file "ko" that exploits the PwnKit vulnerability (CVE-2021-4034) to escalate privileges to the root user. Following successful exploitation, the cryptocurrency miner malware hezb is deployed.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA256	f13e48658426307d9d1434b50fa0493f566ed1f31d6e88bb4ac2ae12ec31ef1f 4dcae1bddfc3e2cb98eae84e86fb58ec14ea6ef00778ac5974c4ec526d3da31f aaa4aaa14e351350fccbda72d442995a65bd1bb8281d97d1153401e31365a3
IPV4	202[.]28[.]229[.]174 199[.]247[.]0[.]216 106[.]251[.]252[.]226:4545
URLs	http[:]//202.28.229.174/ap.txt http[:]//202.28.229.174/kthmimu.txt http[:]//202.28.229.174/sys.x86_64 http[:]//202.28.229.174/ko http[:]//202.28.229.174/ldr.sh http[:]//202.28.229.174/ap.sh http[:]//202.28.229.174/curl http[:]//202.28.229.174/kik

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-26134	Atlassian Confluence Server: 5.0 - 7.18.0	cpe:2.3:a:atlassian:atlassian_confluence_server:*:*:*:*:*:*:*:*	CWE-94
CVE-2021-4034	Polkit versions from 2009	cpe:2.3:a:polkit_project:polkit:*:*:*:*:*:*:*:*	CWE-125 CWE-787 CWE-284

Patch Links

https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

https://gitlab.freedesktop.org/polkit/polkit/-/commit/a2bf5c9c83b6ae46cbd5c779d3055bff81ded683

https://www.debian.org/security/2022/dsa-5059

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.434679

https://www.suse.com/support/update/announcement/2022/suse-su-20220189-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20220190-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20220191-1/

https://www.debian.org/lts/security/2022/dla-2899

https://oss.oracle.com/pipermail/el-errata/2022-January/012089.html

https://oss.oracle.com/pipermail/el-errata/2022-January/012086.html

https://oss.oracle.com/pipermail/el-errata/2022-January/012084.html

References

https://www.trendmicro.com/en_us/research/22/i/atlassian-confluence-vulnerability-cve-2022-26134-abused-for-cryptocurrency-mining-other-malware.html

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

September 22, 2022 . 6:30 AM

More at www.hivepro.com