Hive Pro

THREAT ADVISORY

Cerber targeting organizations with publicly available exploits

TA202158

Threat Level RED

Publish Date – Dec 14, 2021

Cerber, a ransomware that mysteriously vanished in 2019, has reappeared with a new encryption. The new cerber includes fresh source code and makes use of the new library Crypto+++, whereas the previous form made use of Windows CryptoAPI libraries.

Cerber is utilizing following two vulnerabilities:

- CVE-2021-26084: a remote code execution vulnerability that allows an attacker to execute arbitrary code in Atlassian Confluence Servers and Datacenters versions 6.13.22, 6.14.0-7.4.10, 7.5.0-7.11.5, 7.12.0-7.12.4. It has been fixed in versions 6.13.23, 7.4.11, 7.11.6, and 7.12.5.
- CVE-2021-22205: GitHub Gitlab community and enterprise versions 11.9.0-13.8 are affected by a command execution vulnerability that can be exploited by uploading an image that runs via the ExifTool of GitLab Workhorse and achieving remote code execution via a specially designed file. It has been fixed in version 13.9.

The new Cerber ransomware uses either of the two vulnerabilities mentioned above and then enters victims' systems and encrypts their files. Cerber ransomware places the ransom note in the file __$$RECOVERY_README$$__.html, and all the encrypted files have an extension of .locked.

Organizations can patch both vulnerabilities by upgrading their systems to fixed versions.

The TTPs used by Cerber includes:
TA0002 - Execution
T1059 - Command and Scripting Interpreter
T1059.003 - Command and Scripting Interpreter: Windows Command Shell
TA0007 - Discovery
T1012 - Query Registry
T1082 - System Information Discovery

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-26084	Atlassian confluence Servers and Datacenters versions Up to 6.13.22, 6.14.0-7.4.10, 7.5.0-7.11.5, 7.12.0-7.12.4	cpe:2.3:a:atlassian:confluence:*:*:*:*:*:*:*:*, cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*:*:*, cpe:2.3:a:atlassian:data_center:*:*:*:*:*:*:*:*	Atlassian Confluence Server and Center code execution vulnerability	CWE-74
CVE-2021-22205	GitHub Gitlab community and enterprise versions 11.9.0-13.8.7, 13.9.0-13.9.5	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	GitLab command execution vulnerability	CWE-20

Hive Pro

THREAT ADVISORY

Indicators of Compromise(IoCs)

Type	Value
Hash(SHA256)	2ace8c4c98c050a9cf57e0e275848c6cf7122f19f4136dabb94a130a88d77997
Hash(SHA1)	080c62f371a28486e9945ac7ad57c45d8ab6dd00
Hash(MD5)	e278d253cae5bc102190e33f99596966 76ee3782aa050c1b6bf8dd0567f57baa 3c4a05882045e90aab818a5cb8e3a8da
URL	http://128.199.118.202/tmp.sh.2p
IPV4	128.199.118.202

Patch Links

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

References

https://gitlab.com/gitlab-org/gitlab/-/issues/327121
https://packetstormsecurity.com/files/164768/GitLab-Unauthenticated-Remote-ExifTool-Command-Injection.html
https://packetstormsecurity.com/files/164013/Confluence-Server-7.12.4-OGNL-Injection-Remote-Code-Execution.html
https://otx.alienvault.com/pulse/61af78ee529faac40b2de15e/related
https://app.any.run/tasks/c59f562e-4a61-459c-b0a3-9890c412b0ea/
https://www.bleepingcomputer.com/news/security/new-cerber-ransomware-targets-confluence-and-gitlab-servers/