THREAT BULLETINS

US Cyber Command (USCYBERCOM) Issues Warning of Mass exploitation regarding Atlassian Confluence CVE-2021-26084

TLP:WHITE

Sep 03, 2021

On September 3, 2021, USCYBERCOM issued an alert related to mass exploitation of an Atlassian Confluence Server and Data Center vulnerability, CVE-2021-26084. The threat is ongoing and expected to accelerate.

Atlassian Confluence is a popular web-based corporate team workspace designed to help employees collaborate on various projects.

Successful exploitation of this vulnerability could allow an unauthenticated user to execute arbitrary code on a Confluence Server or Data Center instance. Depending on the privileges associated with the instance, an attacker could view, change, or delete data.

On August 25, 2021, Atlassian issued security updates to address the actively exploited Confluence remote code execution (RCE) vulnerability tracked as CVE-2021-26084 and enabling unauthenticated attackers to execute commands on a vulnerable server remotely.

Multiple threat actors began scanning for and exploiting this recently disclosed Confluence vulnerability to install crypto miners after a PoC exploit was publicly released six days after Atlassian's patches were issued.

Cybersecurity intelligence firm Bad Packets also spotted threat actors from multiple countries deploying and launching PowerShell or Linux shell scripts on compromised Confluence servers.

Even though these attackers are currently only deploying cryptocurrency miners, attacks can quickly escalate if the threat actors start moving laterally through corporate networks from compromised on-prem Confluence servers to drop ransomware payloads and exfiltrate data.

Reference(s)	Bleeping Computer, Atlassian, Twitter
Report Source(s)	Government Agency

CVE(s)
CVE-2021-26084

Recommendations
Atlassian recommends that you upgrade to the latest Long Term Support release. For a full description of the latest version, see the Confluence Server and Data Center Release Notes. You can download the latest version from the download centre.

If you are running an affected version upgrade to version 7.13.0 (LTS) or higher.

If you are running 6.13.x versions and cannot upgrade to 7.13.0 (LTS) then upgrade to version 6.13.23.

If you are running 7.4.x versions and cannot upgrade to 7.13.0 (LTS) then upgrade to version 7.4.11.

If you are running 7.11.x versions and cannot upgrade to 7.13.0 (LTS) then upgrade to version 7.11.6.

If you are running 7.12.x versions and cannot upgrade to 7.13.0 (LTS) then upgrade to version 7.12.5.

Confluence Server or Data Center Node running on Linux based Operating System.If you are unable to upgrade Confluence immediately, then as a temporary workaround, you can mitigate the issue by running the script below.

If you run Confluence in a cluster, you will need to repeat this process on each node. You do not need to shut down the cluster.

1. Shut down Confluence.

2. Download the cve-2021-26084-update.sh to the Confluence Linux Server.

3. Edit the cve-2021-26084-update.sh file and set INSTALLATION_DIRECTORY to your Confluence installation directory, for example:
4. INSTALLATION_DIRECTORY=/opt/atlassian/confluence
5. Save the file.
6. Give the script execute permission.
7. chmod 700 cve-2021-26084-update.sh
8. Change to the Linux user that owns the files in the Confluence Installation directory, for example:
9. $ ls -l /opt/atlassian/confluence | grep bindrwxr-xr-x 3 root root 4096 Aug 18 17:07 bin # In this first example, we change to the 'root' user # to run the workaround sudo su root
10. $ ls -l /opt/atlassian/confluence | grep bindrwxr-xr-x 3 confluence confluence 4096 Aug 18 17:07 bin# In this second example, we need to change to the 'confluence' user # to run the workaround script$ sudo su confluence
11. Run the workaround script.
12. $ ./cve-2021-26084-update.sh
13. The expected output should confirm up to five files updated and end with:
14. Update completed!
15. The number of files updated will differ, depending on your Confluence version.
16. Restart Confluence.

Remember, all your nodes.

Confluence Server or Data Center Node running on Microsoft Windows

If you run Confluence in a cluster, you will need to repeat this process on each node. You do not need to shut down the whole cluster.

1. Shut down Confluence.

2. Download the cve-2021-26084-update.ps1 to the Confluence Windows Server.

3. Edit the cve-2021-26084-update.ps1 file and set the INSTALLATION_DIRECTORY.
   Replace Set_Your_Confluence_Install_Dir_Here with your Confluence installation directory, for example:

4. $INSTALLATION_DIRECTORY='C:\Program Files\Atlassian\Confluence'

5. Save the file.

6. Open up a Windows PowerShell (use Run

7. Due to PowerShell's default restrictive execution policy, run the PowerShell using this exact command:

8. Get-Content .\cve-2021-26084-update.ps1 | powershell.exe -noprofile -

9. The expected output should show the status of up to five

10. Update completed!

11. The number of files updated will differ, depending on your Confluence version.

12. Restart Confluence.

Remember, if you run Confluence in a cluster, make sure you run this script on all your nodes.

Sources
References:

https://community.atlassian.com/t5/Confluence-questions/Mining-malware-and-DDOS-attack-to-remote-host-from-Confluence/qaq-p/1794688

https://twitter.com/cnmf_cyberalert/status/1433787671785185283

https://www.bleepingcomputer.com/news/security/us-govt-warns-orgs-to-patch-massively-exploited-confluence-bug/

Alert ID b9292246

View Alert

Tags USCYBERCOM, CVE-2021-26084, Atlassian Confluence

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**