THREAT INTELLIGENCE
SPECIAL ALERT

Special Alert

This alert is of critical importance and thus being sent out ahead of our next Weekly Threat Intelligence Briefing.

Atlassian Confluence Server Vulnerability - CRITICAL

What Happened?

On June 2, 2022, Atlassian posted a security advisory stating that Atlassian Confluence Server software is affected by a zero-day vulnerability that allows attackers to achieve unauthenticated remote code execution. This vulnerability appears to be a command injection vulnerability. This vulnerability, identified as CVE-2022-26134, is trivial to exploit. Currently, Confluence Server version 7.18.0 and all Confluence Data Center versions >= 7.4.0 are affected.

Are you impacted?

CVE-2022-26134 is actively being exploited and has resulted in attackers writing web shells (typically JSP) to publicly accessible web directories. Other post-exploitation activity has been observed in memory only, such as Cobalt Strike or other memory only web shells. Other indicators of compromise include:

- Reconnaissance commands such as "/etc/passwd" and "/etc/shadow"
- Additional web shells written to web directories
- Altering of web access logs

What to Do

Regardless of whether your Confluence Server has been exploited, *it is strongly recommended that external access to Internet-facing Confluence Server be blocked until a patch has been released.* Furthermore, ensure Confluence Server logs are being retained in the event an incident does occur. GreyCastle Security recommends searching these logs for potential indicators of compromise.

If you have identified indicators of compromise on your Confluence Server and need assistance with response, please contact GreyCastle Security’s Incident Response hotline at 800-403-8350 or click the link below.

CONTACT INCIDENT RESPONSE