NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

PATCH CRITICAL VULNERABILITY IN ATLASSIAN CONFLUENCE

DISCUSSION

On March 20, 2019, Atlassian published an advisory about a critical vulnerability (CVE-2019-3396) in its Confluence®[1] Server or Confluence Data Center software that could allow adversaries to execute code remotely on systems running the vulnerable application. Along with the advisory, Atlassian released a software patch to fix the vulnerability[2].

Specifically, there is a server-side template injection vulnerability in the Widget Connector, a macro used by Confluence. Adversaries can exploit this vulnerability in the affected application, without credentials, to gain remote code execution on the system running Confluence.

Both Nation State Advanced Persistent Threat (APT)[3] and criminal actors have exploited this vulnerability with goals ranging from delivering ransomware[4] to gaining control of exploited systems[5]. Any unpatched servers operate at significant risk and it is strongly recommended that they be patched promptly.

MITIGATION ACTIONS

Update Confluence immediately by installing the patch for CVE-2019-3396. Using an older or unpatched version of Confluence makes your system vulnerable to exploitation. Confluence Server and Confluence Data Center versions 6.15.1, 6.14.2, 6.13.3, 6.12.3, and 6.6.12 (and any newer versions) are patched and not vulnerable. You can download the newest versions here:

- https://www.atlassian.com/software/confluence/download (latest build)
- https://www.atlassian.com/software/confluence/download-archives (patches for older builds)
- https://confluence.atlassian.com/doc/upgrading-confluence-4578.html (guidance on upgrading)

For a temporary mitigation of this vulnerability, administrators can disable the Widget Connector and WebDav plugin2. Although this can temporarily reduce functionality, this mitigation will prevent exploitation while updates are prepared. In general, procedures should be in place to patch and update systems and software in a timely manner when vulnerabilities such as this one are announced.

[1] Confluence is a registered trademark of Atlassian

[2] https://confluence.atlassian.com/doc/confluence-security-advisory-2019-03-20-966660264.html

[3] https://fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html

[4] https://blog.alertlogic.com/active-exploitation-of-confluence-vulnerability-cve-2019-3396-dropping-gandcrab-ransomware/

[5] https://www.tenable.com/blog/cve-2019-3396-vulnerability-in-atlassian-confluence-widget-connector-exploited-in-the-wild

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or endorsement purposes.

NOTICE

The information contained in this document was developed in the course of NSA's cybersecurity missions including its responsibilities to identify and disseminate threats to national security systems and Department of Defense information technologies, develop and issue security implementation specifications for cybersecurity-enabled products, and to assist Executive departments and agencies with operational security programs. The information may be shared broadly to reach all appropriate stakeholders.

CONTACT

For general cybersecurity inquiries and reporting, contact the NSA Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov .

For media inquiries, contact Press Desk: 443-634-0721 Email: MediaRelations@nsa.gov