مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Atlassian Confluence Products

Tracking #:432315638

Date:22-02-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a High-Severity Vulnerability in Atlassian Confluence Products, which could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

- **CVE-2024-21678**
- CVSS Base Score: 8.5 HIGH
- A Stored Cross-Site Scripting (XSS) vulnerability exists in Confluence Data Center. An authenticated attacker could exploit this vulnerability to inject arbitrary HTML or JavaScript code into a victim's browser, potentially leading to various malicious activities like stealing sensitive data, compromising user sessions, or redirecting users to malicious websites.

Affected and Fixed Versions:

Confluence Data Center:

- **from 8.7.0 to 8.7.1:** 8.8.0 recommended or 8.7.2
- **from 8.6.0 to 8.6.1:**8.8.0 recommended
- **from 8.5.0 to 8.5.4 LTS:** 8.8.0 recommended or 8.5.5 LTS or 8.5.6 LTS
- **from 8.4.0 to 8.4.5:** 8.8.0 recommended or 8.5.5 LTS or 8.5.6 LTS
- **from 8.3.0 to 8.3.4:** 8.8.0 recommended or 8.5.5 LTS or 8.5.6 LTS
- **from 8.2.0 to 8.2.3:** 8.8.0 recommended or 8.5.5 LTS or 8.5.6 LTS
- **from 8.1.0 to 8.1.4:** 8.8.0 recommended or 8.5.5 LTS or 8.5.6 LTS
- **from 8.0.0 to 8.0.4:** 8.8.0 recommended or 8.5.5 LTS or 8.5.6 LTS
- **from 7.20.0 to 7.20.3:** 8.8.0 recommended or 8.5.5 LTS or 8.5.6 LTS
- **from 7.19.0 to 7.19.17 LTS:** 8.8.0 recommended or 8.5.6 LTS or 7.19.18 LTS or 7.19.19 LTS
- **from 7.18.0 to 7.18.3:** 8.8.0 recommended or 8.5.6 LTS or 7.19.19 LTS
- **from 7.17.0 to 7.17.5:** 8.8.0 recommended or 8.5.6 LTS or 7.19.19 LTS
- **Any earlier versions:** 8.8.0 recommended or 8.5.6 LTS or 7.19.19 LTS

Confluence Server:

- from 8.5.0 to 8.5.4 LTS**: 8.5.5 LTS or 8.5.6 LTS recommended**
- from 8.4.0 to 8.4.5: **8.5.6 LTS recommended**
- from 8.3.0 to 8.3.4: **8.5.6 LTS recommended**
- from 8.2.0 to 8.2.3: **8.5.6 LTS recommended**
- from 8.1.0 to 8.1.4: **8.5.6 LTS recommended**
- from 8.0.0 to 8.0.4: **8.5.6 LTS recommended**
- from 7.20.0 to 7.20.3: **8.5.6 LTS recommended**
- from 7.19.0 to 7.19.17 LTS: **8.5.6 LTS recommended or 7.19.18 LTS or 7.19.19 LTS**
- from 7.18.0 to 7.18.3: **8.5.6 LTS recommended or 7.19.19 LTS**
- from 7.17.0 to 7.17.5: **8.5.6 LTS recommended or 7.19.19 LTS**
- Any earlier versions: **8.5.6 LTS recommended or 7.19.19 LTS**

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Atlassian.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://confluence.atlassian.com/security/security-bulletin-february-20-2024-1354501606.html