مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Ivanti

Tracking #:432316377

Date:09-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Ivanti has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Ivanti has issued security updates to address multiple vulnerabilities in its products including three newly discovered zero-day vulnerabilities in its Cloud Services Appliance (CSA), which are currently being exploited in cyberattacks. The vulnerabilities, identified as CVE-2024-9379, CVE-2024-9380, and CVE-2024-9381, can be exploited in chained with a previously patched zero-day, CVE-2024-8963.
Ivanti has reported that exploitation attempts have primarily targeted customers using CSA 4.6 patch 518 and earlier. Ivanti advises affected customers to upgrade to CSA version 5.0.2 immediately and to rebuild their CSA appliances if they suspect compromise due to these vulnerabilities.

Alongside the CSA vulnerabilities, Ivanti has also patched several other products:

1. **Ivanti Connect Secure and Policy Secure** -(CVE-2024-37404)- 9.1 (Critical)
    - Affected Version(s)-
        - Ivanti Connect Secure- All version before 22.7R2.1
        - Ivanti Policy Secure -All versions before 22.7R1.1
    - Resolved Version(s)-
        - Ivanti Connect Secure -22.7R2.1, 22.7R2.2, 9.1R18.9 (to be released on October 15)
        - Ivanti Policy Secure- 22.7R1.1

2. **Ivanti Endpoint Manager Mobile (EPMM)**-(CVE-2024-7612)- 8.8 (High)
    - Affected Version(s)-12.1.0.3 and prior
    - Resolved Version(s)-12.2+, 12.1.0.4 and 12.0.0.5

3. **Velocity License Server-**(CVE-2024-9167)- 7.0 (High)
    - Affected Version(s)-5.1 versions prior to 5.1.2
    - Resolved Version-5.2

4. **Ivanti Avalanche-**(CVE-2024-47008, CVE-2024-47011, CVE-2024-47007)-7.5 High
    - Affected Version(s)-6.4.2.313 and below
    - Resolved Version-6.4.5

RECOMMENDATIONS:

- Organizations utilizing Ivanti products must prioritize these updates to mitigate risks associated with these vulnerabilities actively exploited in the wild.
- Continuous monitoring and prompt action are essential to safeguard sensitive data and maintain system integrity against potential cyber threats.

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:

- https://www.ivanti.com/blog/october-2024-security-updates