مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Ivanti Products

Tracking #:432316501

Date:13-11-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Ivanti has released critical security updates for various products to address multiple high- and critical-severity vulnerabilities.

TECHNICAL DETAILS:

1. **Ivanti Endpoint Manager (EPM):**
   Notable Vulnerability: CVE-2024-50330 9.8 (Critical): A critical SQL injection vulnerability allows a remote unauthenticated attacker to achieve remote code execution, with no user interaction required.

Affected Versions:
- 2024 September security update and prior
- 2022 SU6 September security update and prior

Fixed Versions:
- 2024 November Security Update
- 2022 SU6 November Security Update

2. **Ivanti Avalanche:**
   Ivanti has released updates for Ivanti Avalanche which addresses five high severity vulnerabilities. Successful exploitation could lead to denial of service to legitimate users or leaking of sensitive information.
   Notable Vulnerabilities: CVE-2024-50317 to CVE-2024-50321 & CVE-2024-50331- 7.5 (High)

Affected Versions:
- Ivanti Avalanche 6.4.5 and prior

Fixed Versions:
- Ivanti Avalanche 6.4.6

3. **Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), Ivanti Secure Access Client (ISAC)**
   Notable Vulnerabilities CVE-2024-38655,CVE-2024-38656, CVE-2024-39710. CVE-2024-39711, CVE-2024-39712, CVE-2024-11007, CVE-2024-11006, CVE-2024-11006- 9.1 Critical

Affected Versions:
- Ivanti Connect Secure-22.7R2.2 and prior
- Ivanti Policy Secure-22.7R1.1 and prior
- Ivanti Secure Access Client-22.7R3 and prior

Fixed Versions:
- Ivanti Connect Secure-22.7R2.3
- Ivanti Policy Secure-22.7R1.2
- Ivanti Secure Access Client-22.7R4

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://forums.ivanti.com/s/article/Security-Advisory-EPM-November-2024-for-EPM-2024-and-EPM-2022?_gl=1*pchng3*_gcl_au*ODM2NTAyMzg1LjE3MjY2NjkwMTg
- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-Multiple-CVEs-Q4-2024-Release?_gl=1*pchng3*_gcl_au*ODM2NTAyMzg1LjE3MjY2NjkwMTg
- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs?_gl=1*6ap9xw*_gcl_au*ODM2NTAyMzg1LjE3MjY2NjkwMTg