مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Ivanti

Tracking #:432317688

Date:10-09-2025

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 that Ivanti has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Ivanti has released security updates to address multiple vulnerabilities in Ivanti Endpoint Manager (EPM), Ivanti Connect Secure, Policy Secure, ZTA Gateways, and Neurons for Secure Access.
These vulnerabilities include missing authorization checks, cross-site request forgery (CSRF), server-side request forgery (SSRF), reflected text injection, and denial-of-service (DoS) flaws. Exploitation could allow attackers to escalate privileges, perform unauthorized actions, achieve remote code execution, or disrupt services.

High Severity Vulnerabilities

- **CVE-2025-55145** – CVSS 8.9: Missing authorization allows remote authenticated attacker to hijack existing HTML5 connections.
- **CVE-2025-55147** – CVSS 8.8: CSRF permits remote unauthenticated attacker to execute sensitive actions with user interaction.
- **CVE-2025-55148** – CVSS 7.6: Missing authorization allows remote authenticated read-only admin to configure restricted settings.
- **CVE-2025-55141** – CVSS 8.8: Missing authorization permits remote authenticated read-only admin to configure authentication.
- **CVE-2025-55142** – CVSS 8.8: Missing authorization permits remote authenticated read-only admin to configure authentication.
- **CVE-2025-9712** – CVSS 8.8: Insufficient filename validation in Ivanti Endpoint Manager allows remote unauthenticated attacker to achieve remote code execution.
- **CVE-2025-9872** – CVSS 8.8: Insufficient filename validation in Ivanti Endpoint Manager allows remote unauthenticated attacker to achieve remote code execution.

Medium Severity Vulnerabilities

- **CVE-2025-8712** – CVSS 5.4: Missing authorization allows remote authenticated read-only admin to change restricted settings.
- **CVE-2025-8711** – CVSS 5.4: CSRF enables remote unauthenticated attacker to perform limited actions with victim interaction.
- **CVE-2025-55146** – CVSS 4.9: Unchecked return value enables remote authenticated admin to trigger denial of service.
- **CVE-2025-55139** – CVSS 6.8: SSRF lets remote authenticated admin enumerate internal services.
- **CVE-2025-55143** – CVSS 6.1: Reflected text injection allows remote unauthenticated attacker to inject arbitrary HTTP response.
- **CVE-2025-55144** – CVSS 5.4: Missing authorization enables remote authenticated read-only admin to configure restricted settings.

Affected Versions

- Ivanti Connect Secure: 22.7R2.8 and earlier
- Ivanti Policy Secure: 22.7R1.4 and earlier
- ZTA Gateways: 22.8R2.2
- Neurons for Secure Access: 22.8R1.3 and earlier

- Ivanti Endpoint Manager: 2022 SU8 Security Update 1 and prior, 2024 SU3 and prior

Fixed Versions:

- Ivanti Connect Secure: Upgrade to 22.7R2.9 or 22.8R2
- Ivanti Policy Secure: Upgrade to 22.7R1.5
- ZTA Gateways: Update to 22.8R2.3-723
- Neurons for Secure Access (Cloud): No customer action required — patches were auto-applied.
- Ivanti Endpoint Manager: Update to 2022 SU8 SR 2, 2024 SU3 SR 1

RECOMMENDATIONS:

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

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/september-2025-security-update