مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in Ivanti Products

Tracking #:432316857

Date:12-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Ivanti Releases Critical Security Updates for Connect Secure, Policy Secure, Ivanti Cloud Services Application and Secure Access Client to Address Multiple High and Critical Severity Vulnerabilities.

TECHNICAL DETAILS:

Ivanti releases critical security updates for connect secure, policy secure, ivanti cloud services application and secure access client to address multiple high and critical severity vulnerabilities. These vulnerabilities, if exploited, could lead to remote code execution, unauthorized access, and exposure of sensitive data.

Key Vulnerabilities:

CVE ID	Description	CVSS Score	Impact	Affected Products
CVE-2024-38657	External control of file name allows admin users to write arbitrary files.	9.1 (Critical)	Arbitrary file write leading to system compromise.	ICS, IPS
CVE-2025-22467	Stack-based buffer overflow allows authenticated users to execute remote code.	9.9 (Critical)	Remote code execution (RCE).	ICS
CVE-2024-10644	Code injection allows admin users to execute remote code.	9.1 (Critical)	Remote code execution (RCE).	ICS, IPS
CVE-2024-47908	OS command injection in the admin web console allows RCE.	9.1 (Critical)	Remote code execution (RCE).	CSA
CVE-2024-13813	Insufficient permissions allow local users to delete arbitrary files.	7.1 (High)	Arbitrary file deletion	ISAC

Affected Products and Versions:

Product Name	Affected Versions	Patched Versions
Ivanti Connect Secure (ICS)	22.7R2.5 and below	22.7R2.6
Ivanti Policy Secure (IPS)	22.7R1.2 and below	22.7R1.3
Ivanti Secure Access Client (ISAC)	22.7R4 and below	22.8R1
Ivanti Cloud Services App (CSA)	5.0.4 and prior	5.0.5

RECOMMENDATIONS:

- Organizations using Ivanti Connect Secure, Policy Secure, Secure Access Client, or Cloud Services Application should prioritize patching these vulnerabilities to mitigate the risk of exploitation.

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-Ivanti-Cloud-Services-Application-CSA-CVE-2024-47908-CVE-2024-11771?language=en_US
- https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs?language=en_US