مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Ivanti Connect SSRF vulnerability- exploited to deploy DSLog backdoor

Tracking #:432315609

Date:13-02-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observes threat actors actively exploiting Ivanti Connect's SSRF vulnerability to deploy the new DSLog backdoor on vulnerable devices.

TECHNICAL DETAILS:

Threat actors are actively exploiting a recently disclosed security flaw impacting Ivanti Connect Secure, Policy Secure, and ZTA gateways to deploy a backdoor codenamed DSLog on vulnerable devices.

Researchers confirmed the successful exploitation critical vulnerability, tracked as CVE-2024-21893 (CVSS: 8.2) in Ivanti Connect Secure, Policy Secure, and ZTA gateway products. The threat actor exploited the server-side request forgery (SSRF) vulnerability affecting the embedded SAML module to deploy the new DSLog backdoor on vulnerable devices. Successful installation of the DSLog backdoor allows threat actors to execute commands on the compromised Ivanti servers remotely.

CVE-2024-21893, which was disclosed by Ivanti late last month alongside CVE-2024-21888, refers to a server-side request forgery (SSRF) vulnerability in the SAML module.

Successful exploitation of the vulnerability could enable threat actors to elevate privileges to an administrator level or access certain restricted resources without authentication.

Affected Versions:
Ivanti Connect Secure 9.x, 22.x
Ivanti Neurons for ZTA All Versions
Ivanti Policy Secure 9.x, 22.x

Fixed Versions:
Ivanti Connect Secure (versions 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2, 22.5R1.1 and 22.5R2.2), Ivanti Policy Secure version 22.5R1.1 and ZTA version 22.6R1.3.

INDICATORS OF COMPROMISE(IoCs):

- Attached in Excel File

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Ivanti.

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors

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://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US
2. https://www.ivanti.com/blog/security-update-for-ivanti-connect-secure-and-ivanti-policy-secure-gateways