مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Ivanti Products

Tracking #:432315752

Date:04-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Ivanti recently released security updates to address multiple vulnerabilities in Ivanti Connect Secure (ICS), (formerly known as Pulse Connect Secure) and Ivanti Policy Secure gateway.

TECHNICAL DETAILS:

Ivanti has released security updates to address four security flaws impacting Connect Secure and Policy Secure Gateways that could result in code execution and denial-of-service (DoS).

Vulnerabilities Details:

CVE	Description	CVSS
CVE-2024-21894	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code	8.2
CVE-2024-22052	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack	7.5
CVE-2024-22053	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory.	8.2
CVE-2024-22023	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS.	5.3

Affected Products:

- All supported versions – Version 9.x and 22.x

Fixed Versions:

- Ivanti Connect Secure: 22.1R6.2, 22.2R4.2, 22.3R1.2, 22.4R1.2, 22.4R2.4, 22.5R1.3, 22.5R2.4, 22.6R2.3, 9.1R14.6, 9.1R15.4, 9.1R16.4, 9.1R17.4 and 9.1R18.5.
- Ivanti Policy Secure: 22.4R1.2, 22.5R1.3, 22.6R1.2, 9.1R16.4, 9.1R17.4 and 9.1R18.5.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the Patches 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://forums.ivanti.com/s/article/New-CVE-2024-21894-Heap-Overflow-CVE-2024-22052-Null-Pointer-Dereference-CVE-2024-22053-Heap-Overflow-and-CVE-2024-22023-XML-entity-expansion-or-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US