Ivanti Releases Security Update for Ivanti Connect Secure and Policy Secure Gateways

Date: 03rd April 2024 | Severity: High

Summary

Vulnerabilities have been discovered in Ivanti Connect Secure (ICS) (formerly known as Pulse Connect Secure) and Ivanti Policy Secure gateways and a patch is available now. These vulnerabilities impact all supported versions – Version 9.x and 22.x (refer to Granular Software Release EOL Timelines and Support Matrix for supported versions).

Attack Vectors

CVE	Description	CVSS	Vector
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	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H
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	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
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	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H
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	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Indicator of Compromise

Not Applicable

Recommendation

There is a patch available now for all supported versions of the product via the standard download portal. We strongly encourage customers to act immediately to ensure they are fully protected.

Patch 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.

Reference Links

https://www.cisa.gov/news-events/alerts/2024/04/04/ivanti-releases-security-update-ivanti-connect-secure-and-policy-secure-gateways

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