CERT-EU

Security Advisory 2024-033

Multiple Vulnerabilities in Ivanti Connect Secure

April 4, 2024 — v1.0

TLP:CLEAR

History:

- *04/04/2024 — v1.0 – Initial publication*

Summary

On April 2, 2024, Ivanti has addressed critical vulnerabilities in its Connect Secure and Policy Secure products, notably **CVE-2024-21894**, allowing unauthenticated attackers to perform remote code execution (RCE) and denial of service (DoS) attacks [1].

Technical Details

The vulnerability tracked as **CVE-2024-21894** is a severe flaw involving a heap overflow in the IPSec component, enabling RCE and DoS without user interaction. Ivanti also fixed additional vulnerabilities [2] potentially leading to DoS attacks [1].

Affected Products

- Ivanti Connect Secure versions prior 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 versions prior 22.4R1.2, 22.5R1.3, 22.6R1.2, 9.1R16.4, 9.1R17.4 and 9.1R18.5.

Recommendations

CERT-EU recommends applying a patch as soon as possible [3].

References

[1] https://www.bleepingcomputer.com/news/security/ivanti-fixes-vpn-gateway-vulnerability-allowing-rce-dos-attacks/

[2] https://forums.ivanti.com/s/article/SA-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

[3] 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