Mphasis
The Next Applied

Scanning Activity for CVE-2024-22024 - XXE Vulnerability in Ivanti Products

Date: 17th March 2024 | Severity: High

Summary

Ivanti has disclosed numerous critical CVEs. The most recent — CVE-2024-22024 — is no different. Although it does not have as high a CVSS score as previous vulnerabilities, CVE-2024-22024 will still likely be a prime target for attackers. The issue is an XXE vulnerability in the SAML component of Ivanti Connect Secure, Policy Secure, and ZTA gateways that allows unauthorized access to restricted resources. Web infrastructure company Akamai said it has observed "significant scanning activity" targeting CVE-2024-22024 starting February 9, 2024.

Attack Vectors

Yutaka Sejiyama, a security researcher at Macnica, shared his Shodan scan results, reporting that as of February 15, 2024, 00:15 UTC, there were 13,636 Ivanti servers that had yet to apply patches for CVE-2024-21893, CVE-2024-21888, CVE-2023-46805, and CVE-2024-21887.

Regarding CVE-2024-22024, which was disclosed and fixed on February 8, 2024, Sejiyama's research shows a global patching percentage of 77.3% as of today, leaving 5,496 servers exposed to the dangerous unauthorized access flaw. Unfortunately, the flaws affecting Ivanti products were disclosed over a short period, giving administrator little time to prepare for applying the patches. This complicates remediation efforts and heightens the risk of Ivanti systems being left vulnerable for prolonged periods, providing threat actors with a large list of potential victims.

Recommendation

The most effective defense will always be to promptly apply the patches provided by the vendor. And to monitor closely on potential scanning activities.

Reference Links

https://www.bleepingcomputer.com/news/security/over-13-000-ivanti-gateways-vulnerable-to-actively-exploited-bugs/

https://thehackernews.com/2024/02/ivanti-pulse-secure-found-using-11-year.htm

Copyright © Mphasis Corporation. All rights reserved.