Ivanti Warns of New Authentication Bypass Vulnerability (CVE-2024-22024)

Vulnerability Bulletins **TLP:WHITE** **Alert Id: 5b6af96b** **2024-02-09 11:29:39**

On February 8, 2024, Ivanti warned of a new authentication bypass vulnerability, identified as CVE-2024-22024, impacting Connect Secure, Policy Secure, and ZTA gateways. Discovery of the new flaw comes as part of Ivanti's ongoing investigation into vulnerabilities impacting the previously mentioned appliances.

The flaw specifically affects a limited number of support versions of Ivanti Connect Secure (version 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2 and 22.5R1.1), Ivanti Policy Secure (version 22.5R1.1), and ZTA (version 22.6R1.3) for which a patch is available here. There is no evidence of the vulnerability being exploited in the wild, as it was found during Ivanti's internal review and testing of code. However, administrators are urged to secure the appliances immediately to ensure full protection.

According to Ivanti, these patches replace prior patches made available on January 31 and February 1, 2024. For supported versions where a patch has not been released, the mitigation provided on January 31, 2024, is effective at blocking a vulnerable endpoint and is available now via Ivanti's standard download portal. The remaining patches for supported versions will be released on a staggered schedule.

Health-ISAC is distributing this report for your situational awareness.

The Ivanti VPN appliances have been heavily targeted, with the first observed instance of cyber activity involving two zero-day vulnerabilities (CVE-2023-46805 and CVE-2024-21887) being exploited in the wild, disclosed on January 10, 2024. The exploitation of these flaws was also addressed in an alert released by Health-ISAC.

Subsequently, a second set of vulnerabilities (CVE-2024-21893 and CVE-2024-21888) were disclosed on January 31, 2024. The first vulnerability tracked as CVE-2024-21893 is a server-side request forgery vulnerability in the gateways' SAML component that enables attackers to bypass authentication and access restricted resources on vulnerable devices. The second flaw, tracked as CVE-2024-21888, affects the gateways' web component, allowing threat actors to escalate privileges to those of an administrator. Out of these two vulnerabilities, CVE-2024-21893 was reported as being actively exploited in the wild.

Now, as part of an ongoing investigation into vulnerabilities impacting Connect Secure, Policy Secure, and ZTA gateways, an additional flaw has been discovered. The vulnerability (CVE-2024-22024) is due to an XXE (XML eXternal Entities) weakness in the gateways' SAML component that lets remote attackers gain access to restricted resources on unpatched appliances in low-complexity attacks without requiring user interaction or authentication.

Mitigations:

There is no evidence of the most recently disclosed vulnerability being exploited in the wild. However, Ivanti urges users to promptly apply the patch for their supported version. A patch is available for Ivanti Connect Secure (versions 9.1R14.5, 9.1R17.3, 9.1R18.4, 22.4R2.3, 22.5R1.2, 22.5R2.3 and 22.6R2.2), Ivanti Policy Secure (versions 9.1R17.3, 9.1R18.4 and 22.5R1.2) and ZTA gateways (versions 22.5R1.6, 22.6R1.5 and 22.6R1.7).

For users of other supported versions, the mitigation guidance released on January 31, 2024, successfully blocks the vulnerable endpoints until the remaining patches are released.

For additional patching guidance, please see recent updates in Ivanti's knowledge base article here.

Reference(s): Bleeping Computer, ivanti, ivanti, ivanti

CVSS Score: 8.3

Sources:

Ivanti: Patch New Connect Secure Auth Bypass Bug Immediately

Security Update for Ivanti Connect Secure and Ivanti Policy Secure Gateways

CVE-2024-22024 (XXE) for Ivanti Connect Secure and Ivanti Policy Secure

Ivanti Knowledge Base

Tags: CVE-2024-22024, Ivanti

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org