

Forum:[Hack Forums](#)

Thread: [Over 5,000 Ivanti Connect Secure Devices Exposed to Critical RCE Vulnerabilities](#)

JoseMar - April 9, 2025, 3:36 am

Over 5,000 Ivanti Connect Secure Devices Exposed to Critical RCE Vulnerabilities

Over 5,113 Ivanti Interface Secure VPN software stay unpatched and helpless to the dynamic misuse of CVE-2025-22457, a basic stack-based buffer overflow vulnerability that empowers inaccessible code execution (RCE).

The following products and versions are vulnerable to CVE-2025-22457: Ivanti Connect Secure 22.7R2.5 and prior

Pulse Connect Secure (End-of-Support) 9.1R18.9 and prior

Ivanti Policy Secure 22.7R1.3 and prior

ZTA Gateways 22.8R2 and prior

A fix is accessible (at first discharged on February 11, 2025) for CVE-2025-22457 in Ivanti Interface Secure. In any case, the counseling states that patches for Ivanti Policy Secure and ZTA Gateways will not be available until April 21, 2025 and April 19, 2025. Beat Interface Secure 9.1x come to End-of-Support on December 31, 2024 and won't be fixed.

The Shadowserver Foundation's later checks uncovered a broad presentation, with gadgets crossing different nations, including the Joined together States, Japan, China, and Australia.

This vulnerability has as already been exploited in the wild by suspected nation-state actors.

Stack-based buffer overflow vulnerability

CVE-2025-22457 is a stack-based buffer overflow vulnerability with a CVSS score of 9.0 that influences different Ivanti items, counting Ivanti Interface Secure (adaptations 22.7R2.5 and earlier), Beat Interface Secure (9.1R18.9 and earlier), Ivanti Approach Secure (22.7R1.3 and earlier), and ZTA Portals (22.8R2 and earlier).

This permits inaccessible, unauthenticated hackers to execute arbitrary code on all these vulnerable devices without requiring client interaction.

When fixed on February 11, 2025, it was at first classified as a non-exploitable item bug. Be that as it may, Ivanti afterward found it was "exploitable through modern means," with proof of dynamic abuse dating back to mid-March 2025.

"The vulnerability is a buffer overflow with characters limited to periods and numbers, it was evaluated and determined not to be exploitable as remote code execution and didn't meet the requirements of denial of service," Ivanti expressed in their advisory.

The outline of the vulnerability is given below:

Nation-State Misuse Campaign

Security analysts at Google's Mandiant have credited the misuse to UNC5221, a suspected China-nexus risk-performing artist with a history of focusing on edge gadgets.

Following effective misuse, analysts watched the sending of two recently recognized malware families: TRAILBLAZE: An in-memory dropper utilized in the beginning contamination stage.

BRUSHFIRE: A detached backdoor outlined for diligent get-to and espionage.

These instruments permit assailants to keep up long-term get to to compromised systems for information exfiltration and intelligence-gathering purposes. The campaign has allegedly focused on organizations over numerous nations and sectors.

The U.S. Cybersecurity and Framework Security Organization (CISA) has included CVE-2025-22457 in its Known Abused Vulnerabilities Catalog, commanding government organizations to take quick action.

For organizations utilizing influenced items, CISA and Ivanti recommend: Conducting danger chasing utilizing Ivanti's Judgment Checker Instrument (ICT).

Performing a manufacturing plant reset for the most elevated level of confidence.

Applying the accessible fix quickly (Ivanti Interface Secure 22.7R2.6).

Disconnecting defenseless Approach Secure and ZTA Doors until patches got to be accessible on April 21 and April 19, respectively.

Revoking and reissuing all certificates, keys, and passwords if compromise is detected.

"For any instances of Ivanti Connect Secure that were not updated by February 28, 2025, to the latest Ivanti patch (22.7R2.6) and all instances of Pulse Connect Secure (EoS), Policy Secure, and ZTA Gateways, CISA urges users and administrators to implement [mitigation] actions," the organization stated.

The Shadowserver Foundation's worldwide check comes about highlight various organizations that stay helpless in spite of accessible patches and dynamic misuse.

With dangerous on-screen characters proceeding to target these gadgets, organizations must prioritize remediation endeavors promptly to anticipate unauthorized get to and potential information breaches.

Don't forget to update and stay safe!?

Additional sources to explore: You can also search directly by CVE on Google for more information:

[*]

https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US

[*]

<https://www.cisa.gov/news-events/alerts/2025/04/04/ivanti-releases-security-updates-connect-secure-policy-secure-zta-gateways-vulnerability-cve-2025>

[*]

<https://www.rapid7.com/blog/post/2025/04/03/etr-ivanti-connect-secure-cve-2025-22457-exploited-in-the-wild/>

Bastille - April 9, 2025, 7:25 am

This is like the third or forth thread I see about Ivanti, sounds to be a rude month for them haha

Thanks for the share :)

JoseMar - April 9, 2025, 7:31 am

(Apr 9, 2025 07:25 AM) Bastille Wrote: [CITE](#) This is like the third or forth thread I see about Ivanti, sounds to be a rude month for them haha

Thanks for the share :)

What I don't understand is why Ivanti plans to release the patch only on April 21. If they already know the vulnerability exists and now the whole world knows about it too, why wait? This is a major security issue, and delaying the fix just increases the risk. It doesn't make sense.

Tyr - April 9, 2025, 9:45 am

(Apr 9, 2025 07:25 AM)Bastille Wrote: [\[CITE\]](#) This is like the third or forth thread I see about Ivanti, sounds to be a rude month for them haha

Thanks for the share :)

I know, it's insane actually. The CVSS is high too.

Shrdw - April 9, 2025, 10:21 am

It's gotten to the point that i laugh when i see this when i see they have all kinds of money yet it takes forever for a patch to be pushed out.