ultraviolet

THREAT REPORT:

Ivanti Vulnerabilities

Services Performed By:
UltraViolet Cyber
Johnathon Moyer
(443) 351-7630
info@uvcyber.com

Published Date:
02/09/2024

Doc ID: ECORP_SUM_07032023_v1.1

Contents

1 Executive Summary

The past 30 days have not been great for Ivanti services. Four vulnerabilities related to Connect Secure have been disclosed throughout the course of the past month. In mid-January, Ivanti initially released a mitigation file for the first two vulnerabilities. By the end of January however, another vulnerability bypassed the original mitigation, allowing for unauthenticated bypass. This vulnerability, combined with a command injection, allows for remote code execution (RCE). As of February 1st, Ivanti had released a patch that fixed all known vulnerabilities up to that point. Instructions for patching the vulnerabilities require that Ivanti devices be factory reset, as well as have their software and configuration files updated to prevent further exploitation.

2 Technical Analysis

The saga began on January 10, 2024, when Ivanti initially fixed an XML configuration issue related to their Connect Secure appliances, formerly known as Pulse Secure. The issue was initially related to two vulnerabilities: CVE-2023-46805, an authentication bypass vulnerability, and CVE-2024-21887, a command injection vulnerability. Then, two days later, Ivanti published instructions on how to perform the necessary factory reset for impacted appliances. On January 14th, the scope was then expanded to include a patch for Ivanti Policy Secure. Following that, Ivanti updated the knowledge base article to disclose a remote arbitrary code execution vulnerability. Finally, on January 31st, Ivanti updated the knowledge base article to add two more vulnerabilities related to the ongoing issue: CVE-2024-21888 and CVE-2024-21893.

On the same day, the Cybersecurity & Infrastructure Security Agency (CISA) released an alert to all organizations to patch the Ivanti vulnerabilities. An emergency directive was put in place for FCEB agencies to patch impacted Ivanti applications that Friday, February 2nd. At the time of the CISA alert, threat actors had already been observed exploiting the Ivanti vulnerabilities, capturing credentials and dropping webshells to further compromise vulnerable networks. On February 8th, Ivanti released an article about a fifth CVE, CVE-2024-22024. The newest CVE is related to an XML external entity vulnerability which impacts SAML in the previous two services and ZTA gateways. The main tool to detect compromise, the external integrity checker tool (ICT), had already been subverted by threat actors, making it more difficult to know whether an intrusion had occurred. For this reason, CISA strongly recommended that all organizations continue monitoring for malicious activity within their networks, even after the Ivanti fixes had been applied.

Security researchers from multiple organizations released a Proof of Concept (PoC) exploit for the Ivanti vulnerabilities between January 16th and 31st, 2024. Based on information from multiple sources, threat actors are looking for one of fourteen vulnerable binaries within the HTTP web server to exploit. If a vulnerability is found, the threat actor could then send an unauthenticated HTTP request to the SAML server, pass XML data to the vulnerable 'xmltooling' binary which was several versions out of date (version 3.0.2, compared to current version 3.4.x), and then carry out a 'Server Side Request Forgery' exploit (SSRF) against the SOAP service. By performing an SSRF exploit, a threat actor could force the device within the victim network to execute a cURL command to download a binary from a server controlled by the threat actor.

The Ivanti VPN application was later revealed to have many old binaries included in their build, some as old as 23 years. Will Dormann posted the following on InfoSec Exchange:

Things on a current Ivanti VPN box:

- curl 7.19.7 2009-11-04 (14 years)
- openSSL 1.0.2n-fips 2017-12-07 (6 years)
- perl 5.6.1 2001-04-09 (23 years)
- psql 9.6.14 2019-06-20 (5 years)
- cabextract 0.5 2001-08-20 (22 years)
- ssh 5.3p1 2009-10-01 (14 years)
- unzip 6.00 2009-04-29 (15 years)

While exploiting these binaries in the past was difficult due to the reduced attack surface of Ivanti's product, unpatched versions of the product may see threat actors exploit vulnerabilities related to these binaries on unpatched boxes soon.

Given that threat actors are looking for exposed binaries to exploit, monitoring network traffic from external sources would help in detecting initial malicious activity. Previously, UV Cyber released a threat report in October 2023 titled "The Evolving Threats Against Web APIs", written by Jacob Wyatt. This report goes over many of the same activities to look out for with relation to the current Ivanti vulnerabilities. We recommend reading this article for additional information .

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- Follow Ivanti's Knowledge Base article for instructions on how to factory reset all impacted devices within your environment
- If UV Cyber does not have access to certain sections of your internal network logs, we recommend your teams monitor internal network activity for 7-zip archiving unusual files, including 'NTDS.dit', taskmgr.exe dumping LSASS processes, lateral RDP movement from Ivanti boxes, and any unusual log deletion activity

5 References

CVE-2024-22024 (XXE) for Ivanti Connect Secure and Ivanti Policy . Retrieved February 9, 2024, from https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure

KB CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887. (2024, January 10). Retrieved February 7, 2024, from https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

Publications - Security Advisories - CERT-EU. (2024, January 31). Retrieved February 7, 2024, from https://cert.europa.eu/publications/security-advisories/2024

Recent SSRF Flaw in Ivanti VPN Products Undergoes Mass. (2024, February 6). Retrieved February 7, 2024, from https://thehackernews.com/2024/02/recently-disclosed-ssrf-flaw-in-ivanti.html

Threat Brief: Multiple Ivanti Vulnerabilities (Updated Feb. 2). (2024, January 16). Retrieved February 7, 2024, from https://unit42.paloaltonetworks.com/threat-brief-ivanti-cve-2023-46805-cve-2024-21887/

Updated: New Software Updates and Mitigations to Defend Against. (2024, January 30). Retrieved February 7, 2024, from https://www.cisa.gov/news-events/alerts/2024/01/30/updated-new-software-updates-and-mitigations-defend-against-exploitation-ivanti-connect-secure-and

Warning: New Malware Emerges in Attacks Exploiting Ivanti VPN. (2024, February 1). Retrieved February 7, 2024, from https://thehackernews.com/2024/02/warning-new-malware-emerges-in-attacks.html

Will Dormann Blog Post (2024, February 05). Retrieved February 7, 2024, from https://infosec.exchange/@wdormann/111880313720252008