www.volexity.com /blog/2024/01/15/ivanti-connect-secure-vpn-exploitation-goes-global/

Ivanti Connect Secure VPN Exploitation Goes Global

⁝ 1/16/2024

January 15, 2024

by Cem Gurkok, Paul Rascagneres, Sean Koessel, Steven Adair, Thomas Lancaster

VOLEXITY // INTELLIGENCE
Ivanti Connect Secure VPN Exploitation Goes Global
• Volexity identifies over 1,700 compromised Ivanti Connect Secure VPN devices worldwide
• Victims spread across nearly all verticals, including military, defense, government, financial & technology
• Webshell with unique key per victim observed
• Vulnerabilities exploited by multiple threat actors

Important: If your organization uses Ivanti Connect Secure VPN and you have not applied the mitigation, then please do that immediately! Organizations should immediately review the results of the built-in Integrity Check Tool for log entries indicating mismatched or new files. As of version 9.1R12, Ivanti started providing a built-in Integrity Checker Tool that can be run as a periodic or scheduled scan. Volexity has observed it successfully detecting the compromises described in this post across impacted organizations. Last week, Ivanti also released an updated version of the external Integrity Checker Tool that can be further used to check and verify systems.

On January 10, 2024, Volexity publicly shared details of targeted attacks by UTA0178 exploiting two zero-day vulnerabilities (CVE-2024-21887 and CVE-2023-46805) in Ivanti Connect Secure (ICS) VPN appliances. On the same day, Ivanti published a mitigation that could be applied to ICS VPN appliances to prevent exploitation of these vulnerabilities.

> Note: It should once again be reiterated that the mitigation does not remedy an active or past compromise. While it is critical that organizations apply this mitigation, it is just as important that they look for signs their ICS VPN appliance has already been compromised and take action if evidence is found.

Since publication of these details, Volexity has continued to monitor its existing customers for exploitation. Volexity has also been contacted by multiple organizations that saw signs of compromise by way of mismatched file detections. Volexity has been actively working multiple new cases of organizations with compromised ICS VPN appliances.

Simultaneously, Volexity also developed a way to scan devices to look for signs of compromise. As result, Volexity has observed two new major findings related to this ongoing activity:

- Exploitation of these vulnerabilities is now widespread. Volexity has been able to find evidence of compromise of **over 1,700 devices** worldwide.
- Additional threat actors beyond UTA0178 appear to now have access to the exploit and are actively trying to exploit devices.

Timeline of Findings

The timeline of findings from earliest observed exploitation to ongoing activity at the time of writing is below:

- **2023-12-03** | Earliest exploitation observed by Volexity.
- **2024-01-10** | Volexity reports details of observed exploitation of CVE-2024-21887 & CVE-2023-46805.
- **2024-01-11** | Volexity discovers evidence that UTA0178 attempts mass exploitation.
- **2024-01-11** | Mandiant reports on their own observations.
- **2024-01-15** | Volexity discloses evidence of mass exploitation and the suspected compromise of at least 1,700 ICS devices.

Victims are globally distributed and vary greatly in size, from small businesses to some of the largest organizations in the world, including multiple Fortune 500 companies across multiple industry verticals, including the following:

- Global government and military departments
- National telecommunications companies
- Defense contractors
- Technology
- Banking, Finance, and Accounting
- Worldwide consulting
- Aerospace, Aviation, and Engineering

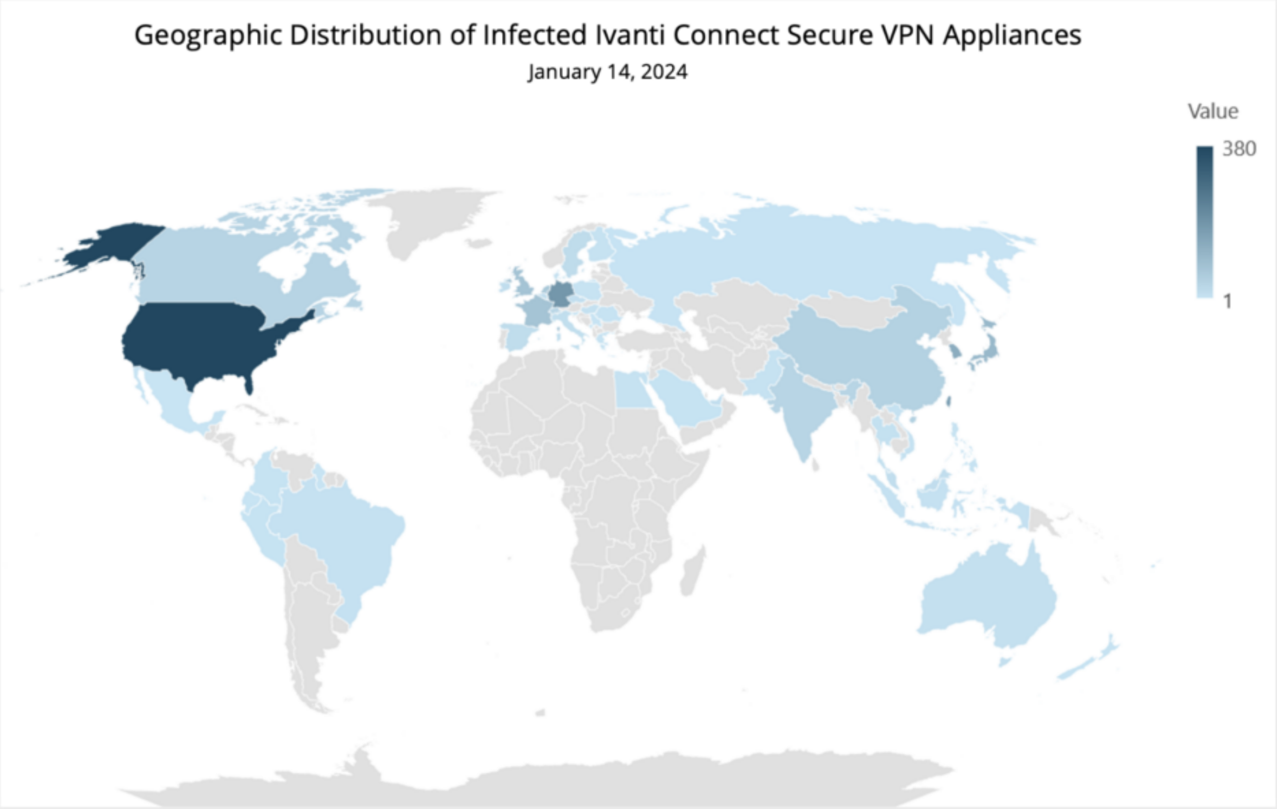
Widespread Exploitation

As described on January 10, 2024, Volexity had conducted scans using a method that only uncovered a single victim organization. Based on those findings, Volexity's customer visibility, and input from Ivanti, it had been concluded that exploitation of the vulnerability chain had been limited to just a few organizations.

However, on January 11, 2024, Volexity began to detect evidence of widespread scanning by someone apparently familiar with the vulnerabilities. Volexity observed various file paths, that are not publicly known, being requested via logs from its customer ICS VPN appliances. It was not clear if this was the work of attackers or security researchers. However, on the same day, Volexity also received reports from multiple organizations that they had received reports of mismatched files from their ICS VPN logs. Further, some of these organizations shared past results from the built-in integrity scan that did not show signs of mismatched files until January 11, 2024. Volexity was simultaneously engaged to investigate similar activity with other customers and found multiple devices had similarly been compromised starting on January 11, 2024.

Investigations of newly found compromised devices showed they had been backdoored with a slightly different variant of the GIFTEDVISITOR webshell documented in the "visits.py modification - GIFTEDVISITOR" section of Volexity's recent blog post. The attacker used an identical webshell to that observed in the first incident investigated by Volexity, but they replaced the AES key used with a truncated UUID string. This AES key format differed from the one initially discovered, which simply had the value `1234567812345678`. Volexity's analysis of multiple devices shows that a unique AES key has likely been employed on each victim system as part of the widespread compromise.

Volexity was able to develop a new method of scanning for evidence that GIFTEDVISITOR was present on ICS VPN appliances. Volexity then scanned roughly 30,000 ICS IP addresses. On Sunday, January 14, 2024, Volexity had identified over 1,700 ICS VPN appliances that were compromised with the GIFTEDVISITOR webshell. These appliances appear to have been indiscriminately targeted, with victims all over the world. A summary of the infected appliances' geography can be seen below.


Geographic Distribution of Infected Ivanti Connect Secure VPN Appliances
January 14, 2024
Value
380
1

Volexity assesses with medium confidence that this widespread exploitation was undertaken by UTA0178. This assessment is based on the use of an identical webshell to that used in the previous exploitation, and the speed at which it was undertaken following publication of details relating to the exploit. Widespread exploitation began taking place January 11, 2024 and continues.

Evidence of Exploit Proliferation

In addition to the discovery of widespread exploitation undertaken by UTA0178, analysis of logs from various ICS VPN appliances showed likely attempted exploitation by other threat actors, with noticeably poorer operational security than UTA0178. While devices without the mitigation did not correctly log exploit-related requests, those with the mitigation correctly log attempted exploitation. Based on analysis of these logs, nearly two dozen IP addresses attempted exploitation using the correct URI pattern or similar URI patterns required for exploitation, with no documentation of this URI pattern in the public domain. These IP addresses appear to be a mix of private VPS instances and compromised network appliances (although no Cyberoam devices have been observed).

Volexity has also observed suspected exploitation attempt from another threat actor that it tracks as UTA0188. This threat actor was observed in the logs of an ICS VPN that was patched. Additional details related to this threat actor, their infrastructure, and other observed targeting were provided to Volexity Threat Intelligence customers in TIB-20240115.

Conclusion

Volexity has identified widespread exploitation of chained vulnerabilities CVE-2024-21887 and CVE-2023-46805. This exploitation has affected thousands of machines and may have infected many more. Volexity's scan methodology would not have worked against organizations that have already deployed the Ivanti mitigation or had otherwise been taken offline. As a result, Volexity suspects there may likely be a higher number of compromised organizations than identified through scanning (which totaled more than 1,700). There was likely a period in which UTA0178 could have actioned these compromises before the mitigation was applied.

Furthermore, Volexity has identified that additional attackers beyond UTA0178 appear to have access to the exploit. Volexity recommends that organizations running ICS VPN perform the following:

- Apply the mitigation provided by Ivanti.
- Run the Integrity Checker Tool provided by Ivanti.
- In the event of a hit for the Integrity Checker Tool, follow the steps in the "Responding to Compromise" section of Volexity's previous blog post.

  Where Volexity has a known contact, national CERTs have been contacted in order to notify them of victims in their constituency. If you are a national CERT, and you have not received a message from Volexity but would like a list of affected IP addresses in your country, please contact threatintel@volexity.com.