Rewterz Threat Advisory - Ivanti VPN Zero-Days Weaponized by UNC5221 Threat Actors to Deploy Multiple Malware Families – Active IOCs - Rewterz

Published: 2024-01-15 · Archived: 2026-04-05 16:13:18 UTC

Severity

High

Analysis Summary

Suspected nation-state threat actors, tracked as UNC5221, have deployed about five different malware families as a part of post-exploitation activities by using two zero-day vulnerabilities in Ivanti Connect Secure (ICS) VPN appliances since at least December 2023.

The malware families used in the attacks help cybercriminals bypass authentication and provide backdoor access to the impacted devices. The threat actors utilize an exploit chain that consists of an authentication bypass vulnerability (CVE-2023-46805) and a code injection flaw (CVE-2024-21887) to take control of the targeted instances.

The two vulnerabilities were used to achieve initial access, backdoor legitimate files, deploy web shells, harvest credentials and other sensitive data, and move further into the infected environment. Ivanti states that the attacks have impacted less than 20 customers, which indicates that this campaign could be targeting specific victims. The patches for these two vulnerabilities are expected to be released during the week of 22nd January.

The analysis by researchers has shown the presence of at least five different custom malware families, aside from the injecting of malicious code into legitimate files inside ICS and the usage of other legitimate tools such as PySoxy and BusyBox to facilitate the follow-up activity. Some parts of the targeted devices are read-only, so UNC5221 leveraged a Perl script (sessionserver.pl) to change the filesystem as read/write allowed the deployment of THINSPOOL, a shell script dropper that can write the web shell LIGHTWIRE to a legitimate Connect Secure file and other subsequent tools.

LIGHTWIRE is one of the two web shells used in the attacks, the other being WIREFIRE. These are lightweight footholds that are made to make sure that persistent remote access is achieved to the infected devices. LIGHTWIRE is written in Perl CGI, whereas WIREFIRE is written in Python. Another malware used in the campaign is a JavaScript-based credential stealer called WARPWIRE and a backdoor dubbed ZIPLINE, capable of uploading and downloading files, creating a proxy server, establishing a reverse shell, and setting up a tunneling server to dispatch traffic between various endpoints.

These attacks do not seem opportunistic but rather intended with a focus on UNC5221’s high-priority targets that it compromised. The threat group has not been attributed to any previously known group and its origins are

currently unknown. However, the targeting of critical infrastructure by weaponization of zero-day vulnerabilities and the use of compromised command-and-control (C2) infrastructure for evading detection indicates that it is an advanced persistent threat (APT).

The activity shows that espionage threat actors find it viable to exploit and live on the edge of networks. The number of impacted systems is very likely to grow too as more organizations run tools to scan their devices for indicators of compromise.

Impact

- Cyber Espionage
- Sensitive Information Theft
- Security Bypass
- Command Execution

Indicators Of Compromise

Domain Name

- symantke.com
- gpoaccess.com
- webb-institute.com

Affected Vendors

Ivanti

Affected Products

- Ivanti ICS 9
- Ivanti ICS 22
- Ivanti Policy Secure

Remediation

- Refer to Ivanti Website for patch, upgrade or suggested workaround information.
- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Implement multi-factor authentication to add an extra layer of security to login processes.
- Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway.
- Organizations need to stay vigilant and follow best practices for cybersecurity to protect their systems and data from potential threats. This includes regularly updating software and implementing strong access

controls and monitoring tools.

- Develop a comprehensive incident response plan to respond effectively in case of a security breach or data leakage.
- Maintain regular backups of critical data and systems to ensure data recovery in case of a security incident.
- Adhere to security best practices, including the principle of least privilege, and ensure that users and applications have only the necessary permissions.
- Establish a robust patch management process to ensure that security patches are evaluated, tested, and applied promptly.
- Conduct security audits and assessments to evaluate the overall security posture of your systems and networks.
- Implement network segmentation to contain and isolate potential threats to limit their impact on critical systems.
