مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerabilities-Ivanti Connect Secure and Ivanti Policy Secure gateways

Tracking #:432315664

Date:01-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways, which are being actively exploited by threat actors.

TECHNICAL DETAILS:

Threat actors are actively exploiting multiple vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways. These can be chained together to allow malicious actors to bypass authentication, craft malicious requests, and execute arbitrary commands with elevated privileges.

Since January 10, 2024, Ivanti has identified five vulnerabilities in its products, four of which have been actively exploited by attackers to deploy malware.

Threat actor tracked as UNC5325 has been observed exploiting CVE-2024-21893 to deploy new malware families such as LittleLamb.WoolTea, PitStop, Pitdog, PitJet, and PitHook.

Two vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways observed being chained to achieve unauthenticated remote code execution (RCE):CVE 2023-46805,CVE-2024-21887 Threat actors exploited the vulnerabilities to implant web shells, including GLASSTOKEN and GIFTEDVISITOR, on internal and external-facing web servers. Once successfully deployed, these web shells are used to execute commands on compromised devices.

After Ivanti provided initial mitigation guidance for CVE 2023-46805, CVE-2024-21887, threat actors developed a way to bypass those mitigations to deploy BUSHWALK, LIGHTWIRE, and CHAINLINE web shell variants. Following the actors' developments, Ivanti disclosed three additional vulnerabilities: CVE-2024-21893, CVE-2024-22024, CVE-2024-21888.

Research reported Ivanti ICT is not sufficient to detect compromise and that a cyber threat actor may be able to gain root-level persistence despite issuing factory resets,

Attackers who exploit one of multiple actively exploited vulnerabilities in Ivanti VPN appliances may be able to maintain root persistence even after a factory reset is performed.

Furthermore, these attackers can also evade detection by Ivanti's internal and external Integrity Checker Tool (ICT) on Ivanti Connect Secure and Policy Secure gateways compromised using the CVE-2023-46805, CVE-2024-21887, CVE-2024-22024, and CVE-2024-21893 exploits.

Vulnerabilities Details:

- **CVE-2023-46805** (High Severity): Authentication bypass vulnerability allowing attackers to access restricted resources without proper authentication.
- **CVE-2024-21887** (Critical Severity): Command injection vulnerability allowing authenticated attackers to execute arbitrary commands on the appliance, potentially granting complete control.
- **CVE-2024-21888** (High Severity): Privilege escalation vulnerability allowing attackers with low privileges to gain higher privileges within the system.
- **CVE-2024-21893** (High Severity): Server-side request forgery (SSRF) vulnerability allowing attackers to perform unauthorized actions on the system.

- **CVE-2024-22024** (High Severity): XML External Entity (XXE) vulnerability allowing attackers with some authentication to access certain restricted resources.

INDICATORS OF COMPROMISE(IOCs):

Refer to this link here for IOCs and More information

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Ivanti.

- Block the IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Implement robust monitoring to detect signs of compromise, focusing on network reconnaissance, lateral movement, and data exfiltration.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b