THREAT ADVISORY

February 1, 2024

Multiple Vulnerabilities in Ivanti Products Could Allow for Remote Code Execution

OVERVIEW

Multiple Vulnerabilities have been discovered in Ivanti Products, the most severe of which could allow for remote code execution.

- Ivanti Connect Secure is a SSL VPN solution for remote and mobile users.
- Ivanti Policy Secure (IPS) is a network access control (NAC) solution which provides network access only to authorized and secured users and devices.
- Ivanti Neurons for Zero Trust Access (nZTA) creates a secure connection from a device to web-based applications on-premises and in the cloud.

Successful exploitation could allow for remote code execution in the context of the system. Depending on the privileges associated with the logged-on user, an attacker could then install programs; view, change, or delete data. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE

According to Ivanti, there have been reports of targeted exploitation of CVE-2024-21893. Ivanti, CISA, and other resources have reported widespread exploitation of CVE-2024-21887, and CVE-2023-46805.

SYSTEMS AFFECTED

- Ivanti Connect Secure (9.x, 22.x)
- Ivanti Policy Secure (9.x, 22.x)
- Ivanti Neurons for ZTA (9.x, 22.x)

RISK

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY

Multiple Vulnerabilities have been discovered in Ivanti Products, the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:

Tactic: *Initial Access* (TA0001):

Technique: *Exploit Public-Facing Application* (T1190):

- A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. This vulnerability can be exploited over the internet. (CVE-2024-21887)
- An authentication bypass vulnerability in the web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. (CVE-2023-46805)
- A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. (CVE-2024-21893)

Tactic: *Privilege Escalation* (TA0004):
Technique: *Exploitation for Privilege Escalation* (T1068):

- A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. (CVE-2024-21888)

CVE-2023-46805 and CVE-2024-21887 can be chained to achieve remote code execution in the context of the system. Depending on the privileges associated with the logged-on user, an attacker could then install programs; view, change, or delete data. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS

We recommend the following actions be taken:

- Apply appropriate updates provided by Ivanti to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5 : Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

- **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
- **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
- **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)

  - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
  - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts:** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. (**M1016**: **Vulnerability Scanning**)

  - **Safeguard 16.13: Conduct Application Penetration Testing:** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

- Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems. (**M1030**: **Network Segmentation**)

  - **Safeguard 12.2: Establish and Maintain a Secure Network Architecture:** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (M1050: Exploit Protection)

  - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

REFERENCES

Ivanti:
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?language=en_US
https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46805
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21887
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21888
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21893