Urgent Security Updates for Ivanti CSA and Connect Secure Vulnerabilities

Overview

Ivanti has issued security updates to resolve multiple high-severity vulnerabilities affecting its Cloud Services Application (CSA) and Connect Secure products. If left unaddressed, these flaws could lead to privilege escalation and remote code execution. Below is a breakdown of the vulnerabilities.

- **CVE-2024-11639** (CVSS 10.0) - Authentication bypass in Ivanti CSA admin web console, allowing remote unauthenticated attackers to gain administrative access.
- **CVE-2024-11772** (CVSS 9.1) - Command injection in Ivanti CSA admin web console, permitting authenticated attackers with admin privileges to execute arbitrary code.
- **CVE-2024-11773** (CVSS 9.1) - SQL injection in Ivanti CSA admin web console, allowing arbitrary SQL execution by authenticated admin users.
- **CVE-2024-11633** (CVSS 9.1) - Argument injection in Ivanti Connect Secure, granting remote code execution to authenticated admin users.
- **CVE-2024-11634** (CVSS 9.1) - Command injection in Ivanti Connect Secure and Policy Secure products, facilitating arbitrary code execution for authenticated admin users.
- **CVE-2024-8540** (CVSS 8.8) - Insecure permissions in Ivanti Sentry, allowing local authenticated attackers to modify sensitive application components.

The vulnerabilities impact the following versions:

- **Ivanti CSA** - Versions before 5.0.3
- **Ivanti Connect Secure** - Versions before 22.7R2.4
- **Ivanti Policy Secure** - Versions before 22.7R1.2
- **Ivanti Sentry** - Versions before 9.20.2, 10.0.2, and 10.1.0

Ivanti is a well-known software company, providing IT management solutions for supply chains, desktop computers, and mobile devices. If these vulnerabilities are exploited, attackers could gain unauthorized administrative access, execute arbitrary commands, or manipulate sensitive data. This could lead to data breaches and disrupt essential services depending on the industry impacted. Aspire recommends patching immediately.

Aspire Protects

- **Patch**
  - See patch guidance for CVE-2024-11639, CVE-2024-11772, and CVE-2024-11773 in Ivanti's advisory.
  - See patch guidance for CVE-2024-1163 and CVE-2024-11634 in Ivanti's advisory.

  - See patch guidance for CVE-2024-8540 in Ivanti's advisory.
- Limit admin privileges to reduce the risk of exploitation.
- Watch for unusual traffic that may indicate attempted exploitation.
- Use network segmentation, multi-factor authentication (MFA), and endpoint protection to minimize exposure.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190) – Attackers may target exposed admin web consoles of CSA or Connect Secure.

Privilege Escalation

- Abuse Elevation Control Mechanism (T1548.002) – Exploiting command and argument injection vulnerabilities to elevate privileges.

Execution

- Command and Scripting Interpreter (T1059) – Leveraging injected commands to execute malicious payloads.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The vulnerabilities in Ivanti CSA and Connect Secure products could impact a broad range of industries due to the widespread use of these solutions for secure remote access, network management, and endpoint security. Industries potentially affected by the vulnerabilities due to the use of file transfer systems:

- Financial Services
- Government
- Retail
- Education
- Technology and Telecommunications
- SMBs

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

- Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
- Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

December Security Update | Ivanti

Security Advisory Ivanti Cloud Services Application (CSA) (CVE-2024-11639, CVE-2024-11772, CVE-2024-11773)

December 2024 Security Advisory Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) (Multiple CVEs)

Security Advisory Ivanti Sentry (CVE-2024-8540)