Critical Siemens Siveillance Video Vulnerability Allows Remote Code Execution

Author: *Portia S. Cole – CTI Researcher*

TL;DR

There is a critical vulnerability (CVE-2026-3014, CVSS 9.1) in Siemens Siveillance Video Management Servers that allows a user with edit permissions to remotely execute arbitrary code through the Management Server API. The code runs under the Management Server Service account.

This is not an unauthenticated vulnerability, but an attacker who compromises a sufficiently privileged account could use it to take control of the server.

Overview

There is a critical vulnerability (CVE-2026-3014, CVSS 9.1) in Siemens Siveillance Video Management Servers caused by operating system command injection in the Management Server API. An attacker with edit permissions can exploit the vulnerability over the network to execute arbitrary code as the Management Server Service. No user interaction is required.

Siemens Siveillance Video is an IP video management platform that centrally manages cameras, servers, storage, users and other connected security devices. It supports deployments ranging from small sites to large, high-security environments.

Affected Products

- Siemens Siveillance Video V2023 R3 versions earlier than V23.3 HotfixRev27
- Siemens Siveillance Video V2024 R1 versions earlier than V24.1 HotfixRev16
- Siemens Siveillance Video V2025 versions earlier than V25.1 HotfixRev15

The impact depends on the permissions assigned to the service account. Successful exploitation could allow an attacker to access video management data, alter system configurations, disrupt management functions or establish a foothold on the internal network. There are no reports of active exploitation, and no public proof-of-concept exploit has been identified.

Impact on Aspire Customers

For Aspire customers, the main concern is losing visibility at locations monitored through Siveillance Video. This could affect campus security, government facilities, retail loss prevention and manufacturing operations.

Finance, legal and professional services may also rely on video recordings to investigate unauthorized access or other incidents. Any interruption could delay the security team's response or leave gaps in the evidence available afterward.

Aspire Protects

- **Patch** – Update Siveillance Video V2023 R3 to V23.3 HotfixRev27 or later.
- Update Siveillance Video V2024 R1 to V24.1 HotfixRev16 or later.
- Update Siveillance Video V2025 to V25.1 HotfixRev15 or later.
- Restrict network access to the Management Server and its API to authorized administrative systems. Do not expose management interfaces directly to the internet.
- Review accounts and roles with edit permissions. Remove access that is no longer required.
- Ensure the Management Server Service account has only the operating system and network permissions needed to perform its functions.
- Monitor for unusual API activity, configuration changes or logins involving accounts with edit permissions.
- Investigate unexpected command shells, script interpreters, file creation or outbound connections initiated by the Management Server Service.
- If updates cannot be applied immediately, place the Management Server behind additional firewall or access control restrictions. These measures reduce exposure but do not fix the vulnerability.

TTPs to Watch

Initial Access

- Valid Accounts [T1078] – An attacker may use a compromised account with edit permissions to access the Management Server API.

Execution

- Command and Scripting Interpreter [T1059] – An attacker may inject operating system commands through the Management Server API to execute arbitrary code.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – An attacker may exploit the vulnerability to execute code with the privileges of the Management Server Service account.

IoCs

There are no known IoCs 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

Organizations using affected Siemens Siveillance Video versions may be at risk, including:

- Public Sector
- Energy
- Legal & Professional Services
- Healthcare
- Finance
- Education
- Retail
- Manufacturing

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

SSA-825228