AL2026_09 Interlock Ransomware Exploits Cisco Secure FMC Zero-Day in Active Attacks (March 23rd, 2026)

Description

Security researchers have reported that the **Interlock ransomware** operation has been exploiting a critical vulnerability in Cisco Secure Firewall Management Center (FMC) software as a zero-day in active attacks since January 2026.

The flaw, tracked as **CVE-2026-20131**, allows unauthenticated attackers to execute arbitrary code remotely on vulnerable systems. The vulnerability affects the web-based management interface used to administer Cisco enterprise firewall appliances.

According to threat intelligence research, the Interlock ransomware group began exploiting the vulnerability weeks before it was publicly disclosed and patched, giving attackers a significant advantage over defenders.

Compromise of Cisco firewall management infrastructure poses a serious risk because these systems often control network security functions such as intrusion prevention, malware protection, and traffic filtering across enterprise networks.

Attack Details

The campaign involves the exploitation of a critical software vulnerability to gain unauthorized access to enterprise network infrastructure.

Key characteristics include:

- **Vulnerability:** CVE-2026-20131, a maximum-severity vulnerability affecting Cisco Secure Firewall Management Center (FMC).
- **Root cause:** The flaw results from insecure deserialization of a user-supplied Java byte stream in the web-based management interface.
- **Remote code execution:** A successful exploit allows an unauthenticated attacker to execute arbitrary Java code with **root privileges** on the affected device.
- **Zero-day exploitation:** Threat intelligence reports indicate that attackers began exploiting the vulnerability as early as **January 26, 2026**, approximately **36 days before public disclosure**.

- **Threat actor:** The **Interlock ransomware** group, a financially motivated cybercrime operation first identified in 2024 and linked to multiple ransomware campaigns targeting organizations worldwide.
- **Potential impact:**
  - Unauthorized administrative access to network security infrastructure.
  - Deployment of ransomware or additional malware within enterprise networks.
  - Data exfiltration and disruption of critical systems.

Because firewall management systems often have broad administrative privileges and visibility across networks, successful exploitation could enable attackers to bypass security controls and pivot deeper into internal environments.

Remediation

Organizations using Cisco firewall management infrastructure should take the following actions immediately:

- **Apply security updates:** Install the latest patches released by Cisco addressing CVE-2026-20131 and related vulnerabilities.
- **Review Cisco security advisories:** Follow vendor guidance and mitigation steps provided in Cisco's official security bulletin.
- **Restrict management access:** Limit access to firewall management interfaces to trusted internal networks and authorized administrators only.
- **Monitor administrative activity:** Review logs for unusual authentication attempts, configuration changes, or suspicious administrative actions on firewall management systems.
- **Network segmentation:** Ensure firewall management servers are isolated from general enterprise networks to limit the impact of compromise.
- **Threat hunting:** Conduct proactive scans and forensic analysis for indicators of compromise (IOCs) associated with Interlock ransomware activity.
- **Backup and recovery planning:** Maintain secure, offline backups and ensure incident response plans include procedures for ransomware recovery.
- **Security monitoring:** Deploy endpoint detection and network monitoring tools capable of detecting suspicious behavior within network management infrastructure.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Gatlan, S. (2026). *Interlock ransomware exploited Secure FMC flaw in zero-day attacks since January.* Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/interlock-ransomware-exploited-secure-fmc-flaw-in-zero-day-attacks-since-january/