AL2025_07 Critical Cisco ISE Vulnerabilities Allow Attackers to Execute Commands as Root (11th February 2025)

Description

Cisco has released patches for two critical vulnerabilities in its Identity Services Engine (ISE) security policy management platform. These vulnerabilities, identified as CVE-2025-20124 and CVE-2025-20125, can be exploited by authenticated remote attackers with read-only admin privileges. If successfully exploited, attackers could execute arbitrary commands with root-level privileges and bypass authorization controls. These flaws affect all Cisco ISE and Cisco ISE Passive Identity Connector (ISE-PIC) appliances, regardless of their configuration. Admins are strongly advised to apply the necessary patches to mitigate potential risks.

Attack Details

CVE-2025-20124

This vulnerability is due to the insecure deserialization of user-supplied Java byte streams by affected software. Attackers can exploit this flaw by sending a crafted serialized Java object to a vulnerable API. If successfully executed, this attack would allow an attacker to run arbitrary commands on the system and escalate privileges to root. This could lead to full system compromise, enabling the attacker to modify configurations, steal sensitive data, or use the compromised system to launch further attacks within the network.

CVE-2025-20125

This vulnerability arises from a lack of proper authorization checks and insufficient validation of user-supplied data. Exploitation involves sending maliciously crafted HTTP requests to an affected API. If successfully exploited, an attacker could obtain sensitive information, modify the system’s configuration, and even trigger a reload of the vulnerable appliance. This could potentially disrupt network operations and compromise security policies, allowing unauthorized access and further exploitation.

Remediation

Cisco has provided fixed releases for affected software versions. Administrators are advised to upgrade to the following patched versions:

Cisco ISE Software Releases	First Fixed Release
3.0	Migrate to a fixed release
3.1	3.1P10
3.2	3.2P7
3.3	3.3P4
3.4	Not vulnerable

Additional Recommendations:

- Restrict access to Cisco ISE management interfaces to trusted networks.
- Implement robust monitoring to detect unauthorized API access attempts.
- Regularly review and apply security patches for Cisco appliances.
- Follow Cisco's official security advisories for future updates and mitigations.

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

References

- Cisco Identity Services Engine insecure Java deserialization and Authorization Bypass vulnerabilities. Retrieved from Cisco (2025, February 6). https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multivuls-FTW9AOXF
- Gatlan, S. (2025, February 6). Critical Cisco ISE bug can let attackers run commands as root. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/critical-cisco-ise-bug-can-let-attackers-run-commands-as-root/