February 23, 2024

Overall rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in the OLE2 file format parser of ClamAV. The vulnerability affects Cisco Secure Endpoint Connector for Windows versions prior to 7.5.17 (Feb 2024)1, 8.2.3.30119 and Secure Endpoint Private Cloud versions prior to 3.8.0 with updated connectors.

Technical Details

A vulnerability in the OLE2 file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability affects only Windows-based platforms because those platforms run the ClamAV scanning process as a service that could enter a loop condition, which would consume available CPU resources and delay or prevent further scanning operations.

This vulnerability is due to an incorrect check for end-of-string values during scanning, which may result in a heap buffer over-read. An attacker could exploit this vulnerability by submitting a crafted file containing OLE2 content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software and consuming available system resources.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** risk. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-20290
- ClamAV OLE2 File Format Parsing Denial of Service Vulnerability
- ClamAV 1.3.0 feature release and 1.2.2, 1.0.5 security patch release!
- VRM Vulnerability Reports