Reducing the Risk of SNMP Abuse | CISA

Published: 2017-06-05 · Archived: 2026-04-05 23:38:28 UTC

Systems Affected

SNMP enabled devices

Overview

The Simple Network Management Protocol (SNMP) may be abused to gain unauthorized access to network devices. SNMP provides a standardized framework for a common language that is used for monitoring and managing devices in a network.

This Alert provides information on SNMP best practices, along with prevention and mitigation recommendations.

SNMP depends on secure strings (or “community strings”) that grant access to portions of devices’ management planes. Abuse of SNMP could allow an unauthorized third party to gain access to a network device.

SNMPv3 should be the only version of SNMP employed because SNMPv3 has the ability to authenticate and encrypt payloads. When either SNMPv1 or SNMPv2 are employed, an adversary could sniff network traffic to determine the community string. This compromise could enable a man-in-the-middle or replay attack.

Although SNMPv1 and SNMPv2 have similar characteristics, 64-bit counters were added to SNMPv2 so it could support faster interfaces. SNMPv3 replaces the simple/clear text password sharing used in SNMPv2 with more securely encoded parameters. All versions run over the User Datagram Protocol (UDP).

Simply using SNMPv3 is not enough to prevent abuse of the protocol. A safer approach is to combine SNMPv3 with management information base (MIB) whitelisting using SNMP views. This technique ensures that even with exposed credentials, information cannot be read from or written to the device unless the information is needed for monitoring or normal device re-configuration. The majority of devices that support SNMP contain a generic set of MIBs that are vendor agnostic. This approach allows the object identifier (OID) to be applied to devices regardless of manufacturer.

Impact

A remote attacker may abuse SNMP-enabled network devices to access an organization’s network infrastructure.

Solution

A fundamental way to enhance network infrastructure security is to safeguard networking devices with secure configurations. US-CERT recommends that administrators:

- Configure SNMPv3 to use the highest level of security available on the device; this would be *authPriv* on most devices. *authPriv* includes authentication and encryption features, and employing both features

enhances overall network security. Some older images may not contain the cryptographic feature set, in which case *authNoPriv* needs to be used. However, if the device does not support Version 3 *authPriv*, it should be upgraded.

- Ensure administrative credentials are properly configured with different passwords for authentication and encryption. In configuring accounts, follow the principle of least privilege. Role separation between polling/receiving traps (reading) and configuring users or groups (writing) is imperative because many SNMP managers require login credentials to be stored on disk in order to receive traps.
- Refer to your vendor's guidance for implementing SNMP views. SNMP view is a command that can be used to limit the available OIDs. When OIDs are included in the view, all other MIB trees are inherently denied. The SNMP *view* command must be used in conjunction with a predefined list of MIB objects.
- Apply extended access control lists (ACLs) to block unauthorized computers from accessing the device. Access to devices with read and/or write SNMP permission should be strictly controlled. If monitoring and change management are done through separate software, then they should be on separate devices.
- Segregate SNMP traffic onto a separate management network. Management network traffic should be out-of-band; however, if device management must coincide with standard network activity, all communication occurring over that network should use some encryption capability. If the network device has a dedicated management port, it should be the sole link for services like SNMP, Secure Shell (SSH), etc.
- Keep system images and software up-to-date.

References

The Interfaces Group MIB using SMIv2

Revisions

June 5, 2017: Initial Release
