Attackers Continue to Target Legacy Devices

By Omar Santos

Published: 2020-10-20 · Archived: 2026-04-05 22:45:51 UTC

Attackers will always target the "low hanging fruit": devices that have passed end-of-software maintenance and end-of-support. A few years ago, Cisco described the evolution of attacks against infrastructure devices. All of the attacks discussed in that article targeted devices that have reached the end-of-sale milestone for several years! Too many organizations are relying on seriously outdated network components and operating systems—thus providing even more opportunity for adversaries to infiltrate or attack their network. In fact, some organizations continue to run network infrastructure software versions that are more than 8 years old (which likely are exposed to many unpatched known vulnerabilities).

Adversarial Tactics and Techniques

The malware used in the aforementioned evolved Cisco IOS attacks show increasing levels of complexity in the type of modifications made to legacy Cisco IOS, the behavior of Command and Control (C2) communication, and the platforms they target. The following are some of the most noticeable tactics and techniques used by adversaries in those attacks:

- Automated exfiltration via traffic duplication by using modified SPAN ports.
- Weaken encryption: Diffie-Hellman keyspace was reduced by attackers.
- Legacy Cisco IOS Software was modified to disable crypto hardware acceleration.
- The ROMMON on the targeted Cisco device was modified to ensure persistence of the command and control channel.
- Attackers leveraged modified ROMMON code in order to inject binary code into the in-memory Cisco IOS image to support data exfiltration.
- The usage of adversary-controlled TFTP servers in order to load malicious software to the targeted infrastructure device.
- Attackers used the Simple Network Management Protocol (SNMP) with stolen credentials to retrieve the compromised device configuration.
- Attackers exfiltrated device-specific data via ICMP packets.
- Crafted ICMP packets were also used to trigger unwanted device behavior that helped the attacker to further manipulate the compromised device.
- Some of the modified software images included keylogging mechanisms designed to capture the network administrator keystrokes.

The Cisco PSIRT has also seen multiple attacks against legacy protocols, such as Smart Install. According to Shodan, there are thousands of devices that are still running Smart Install. Cisco Smart Install is a legacy feature that provides zero-touch deployment for new switches, typically access layer switches. Customers who are

seeking more than zero-touch deployment should consider deploying the Cisco Network Plug and Play solution instead.

The main weakness of the Smart Install protocol is the lack of authorization or authentication mechanisms in between the client and the director. This can allow a client to process crafted Smart Install protocol messages as if these messages were from the Smart Install director. The following are some of the techniques used by attackers leveraging Smart Install enabled devices:

- Attackers changed the TFTP server address on integrated branch clients (IBC).
- Attackers copied arbitrary files from the affected device to an attacker-controlled TFTP server
- The target device's startup configuration (startup-config) file was replaced with a file that the attacker prepared. Attackers then forced a reload of the IBC after a defined time interval; subsequently, booting with the new startup-config.
- In some cases, adversaries loaded attacker-supplied firmware onto the compromised device.
- Attackers were able to execute high-privileged CLI commands on the affected device (including do-exec CLI commands).

A Call to Action

Upgrading infrastructure devices is a big undertaking and in some cases requires network downtime. However, the costs of ignoring the problem of aging infrastructure and running legacy protocols can run much higher. Modern network infrastructure devices now come with numerous security features and capabilities that mitigate all the aforementioned attacks. The Cisco Secure Development Lifecycle (SDL) applies industry-leading practices and technology to build trustworthy solutions that have fewer field-discovered product security incidents. Because network infrastructure devices play a fundamental role in the growth and trajectory of a business, forward-looking leaders and engineers must have a resilience strategy that includes investing in updating IT infrastructure.
