Operation Zero Disco: Attackers Exploit Cisco SNMP Vulnerability to Deploy Rootkits

⋮ 10/14/2025

Exploits & Vulnerabilities

Trend™ Research has uncovered an attack campaign exploiting the Cisco SNMP vulnerability CVE-2025-20352, allowing remote code execution and rootkit deployment on unprotected devices, with impacts observed on Cisco 9400, 9300, and legacy 3750G series.

By: Dove Chiu, Lucien Chuang Oct 15, 2025 Read time: 7 min (1827 words)

Key takeaways:

- Attackers exploited the Cisco SNMP vulnerability (CVE-2025-20352) to deploy Linux rootkits on older, unprotected systems, allowing remote code execution (RCE) and persistent unauthorized access by setting universal passwords and installing hooks into IOSd memory space.
- The operation primarily impacted Cisco 9400, 9300, and legacy 3750G series devices, with additional attempts to exploit a modified Telnet vulnerability (based on CVE-2017-3881) to enable memory

access.
- Trend Vision One™ detects and blocks the IoCs discussed in this blog. Trend Micro customers can also access tailored hunting queries, threat insights, and intelligence reports to better understand and proactively defend against this campaign. In addition, Trend customers are protected from the Cisco SNMP vulnerability exploits via the specific rules and filters listed at the end of this blog entry.

Trend™ Research has detected an operation where attackers exploited a Cisco Simple Network Management Protocol (SNMP) vulnerability to install a rootkit on vulnerable network devices. The SNMP exploit referenced in Cisco's latest advisory is CVE-2025-20352, which affects both 32-bit and 64-bit switch builds and can result in remote code execution (RCE). Trend Research investigation also found that attackers used spoofed IPs and Mac addresses in their attacks.

Trend investigation revealed that once a Cisco device has a rootkit implanted, the malware sets a universal password that includes the word "disco" in it, which Trend Research believes is a one-letter change from Cisco. The malware then installs several hooks onto the IOSd, which results in fileless components disappearing after a reboot. Newer switch models provide some protection via Address Space Layout Randomization (ASLR) which reduces the success rate of intrusion attempts; however, it should be noted that repeated attempts can still succeed.

Trend Micro telemetry has, as of writing, detected that Cisco 9400 series and 9300 series are affected by this operation. The operation also affected Cisco 3750G devices with no guest shell available, but this type of device has already been phased out. Cisco also contributed to this research by providing forensics for their products and impact data, that assisted the Trend investigation.

The operation also attempted to exploit a Telnet vulnerability that is a modified version of CVE-2017-3881. The CVE-2017-3881 vulnerability was also known to be exploited to cause RCE, but the attempts of the attackers modified it to enable memory read/write.

Exploit investigation

Trend investigation recovered several exploits from a compromised Linux attack that targeted both 32-bit and 64-bit platforms.

32-bit

- SNMP exploit capable of installing a rootkit

Network captures show that the exploit traffic targeted a 3750G SNMP service; unfortunately, the exploit code was not fully recovered. Figure 1 shows a malicious SNMP packet we captured in the wild that reveals part of the hacker's command, "*$(ps -a*": investigation suggests that due to the exploit limit, the hacker can only send few bytes of command per SNMP packet, so the whole command is split into several SNMP packets.

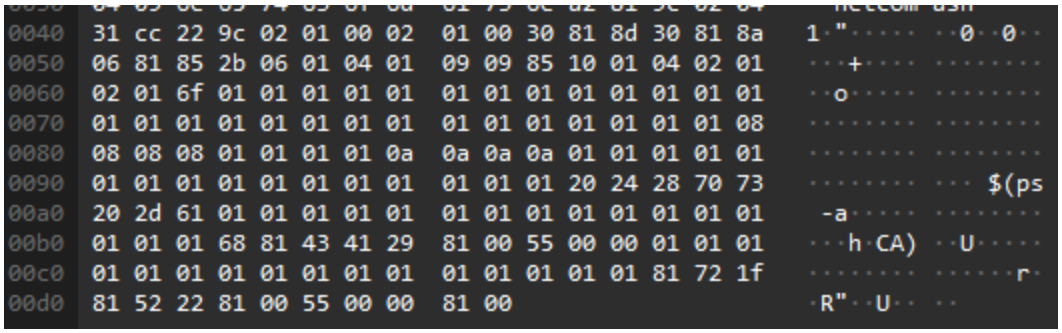

Figure 1. The malicious SNMP packet with the command “$(ps -a”

- Telnet exploit

Investigation confirmed that the Telnet exploit was abused to allow memory read/write at arbitrary addresses, but full functionality is unknown as of writing.

64-bit

- SNMP exploit capable of installing a rootkit

The SNMP exploit that was abused to access 64-bit switch builds required the attacker to be able to run guest shell on the Cisco device; this needs level 15 privilege. If successful, the attacker can log in using the universal password and install a fileless backdoor. After that, the attacker can uses a UDP controller to perform various operations.

- SNMP exploit that can completely stop trace logging on the target

This exploit does not use mmap; the attacker only needs to obtain a few addresses for the exploit to become RCE.

- SNMP exploit with unknown functionality

Trend investigation also found a UDP controller component used to control the rootkit, and an arp spoofing tool on a Cisco switch.

The UDP controller provides several powerful management functions: it can toggle log history on or off or delete log records entirely; bypass AAA authentication and bypass VTY access-control lists; enable or disable a universal password; conceal portions of the running configuration; and reset the timestamp of the last running-config write so the configuration appears never to have been changed.

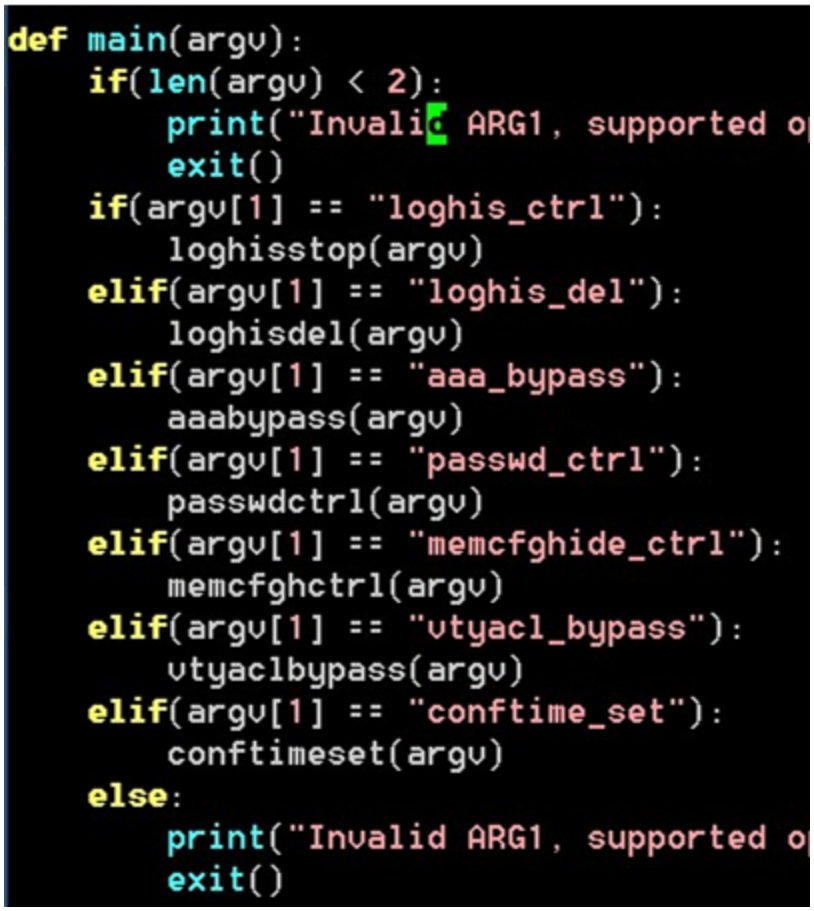

Figure 2. The UDP controller providing several powerful management functions

Attack scenario

Figure 2 shows a diagram of a simulated network where each zone is separated by a core switch and a different VLAN. For management, SSH or RDP are only allowed from a designated waystation and onto servers controlled by an internal firewall. Meanwhile, an external firewall protects all zones. The victim in this scenario uses SNMP to monitor the status of each switch, wherein the SNMP community is public by default on each router.

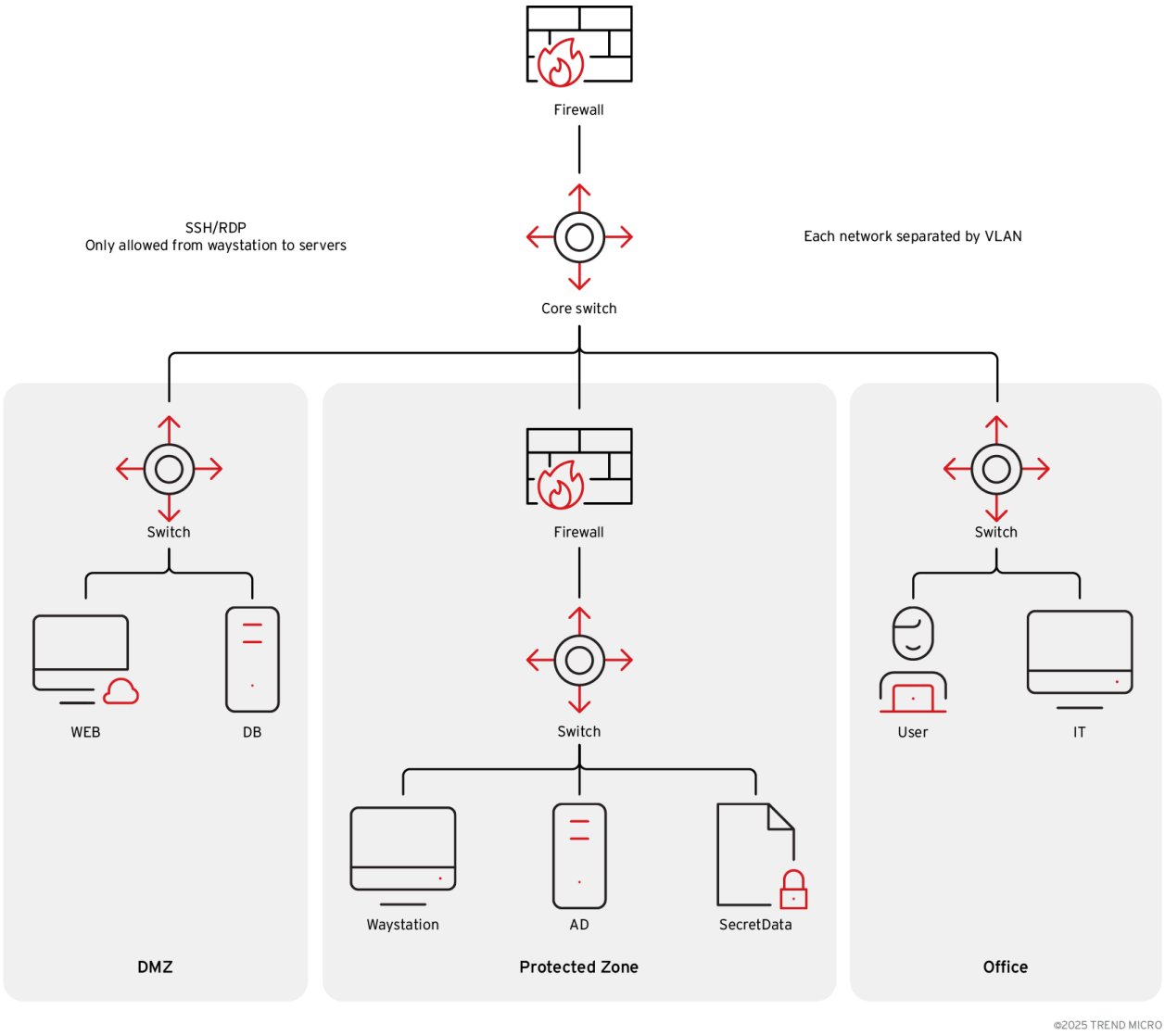

Figure 3. A diagram of a simulated network where where each zone is separated by a core switch and a different VLAN

download

In this simulation, let's assume the attacker has obtained network details such as critical passwords to access different devices on the network. The attacker is aware that they must bypass the external firewall to enter the protected zone, while the internal firewall only allows SSH from waystations. Since all switches are using an SNMP that is set to public by default, this can be the attacker's way in. By exploiting this vulnerability, the attacker could potentially also get privileged access to critical switches and core switches.

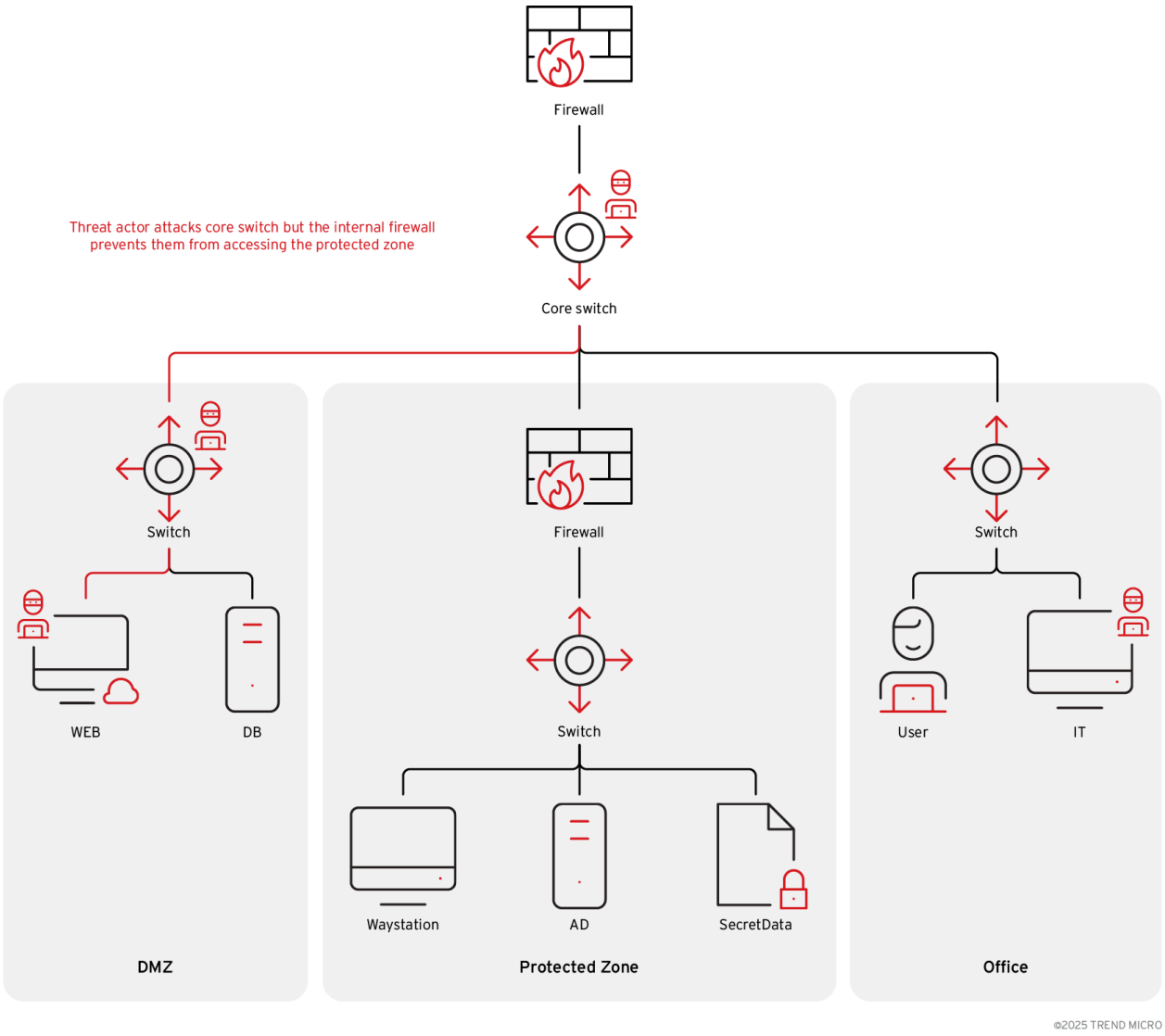

Figure 4. In the simulation, the attacker might be able to bypass the external firewall with obtained passwords to access different devices on the network.
download

Once the attacker gains access to a core switch, they can connect to different VLANs by adding routing rules. However, this is not enough to bypass the internal firewall, so they impersonate a waystation's IP address to bypass the internal firewall. To do this, the attacker:

1. Disables the core switch log remotely
2. Logs in to the core switch
3. Assigns the waystation IP on the port which connects to protected zone
4. Does arp spoofing on that port to redirect the old waystation IP to the core switch, which results in the original waystation becoming offline due to an IP address conflict or mismatch

The arp spoofing tools on Cisco is a Linux elf binary, which can be run on the Cisco guest shell to perform the arp spoofing.

```
}
if ( cheatip && targetip && fakemac && targetmac )
{
  init_device();
  while ( 1 )
  {
    arp_cheat(targetmac, targetip, cheatip, fakemac);
    _sleep(5);
  }
}
IO_puts("check error ");
exit(0xFFFFFFFFLL);
```

Figure 5. The arp spoofing tool

Once the attacker has set up a different IP address and successfully bypasses the internal firewall, they gain access to the protected zone. The attacker then evades detection by recovering the settings on the core switch upon log out and reopens the log functionality remotely.

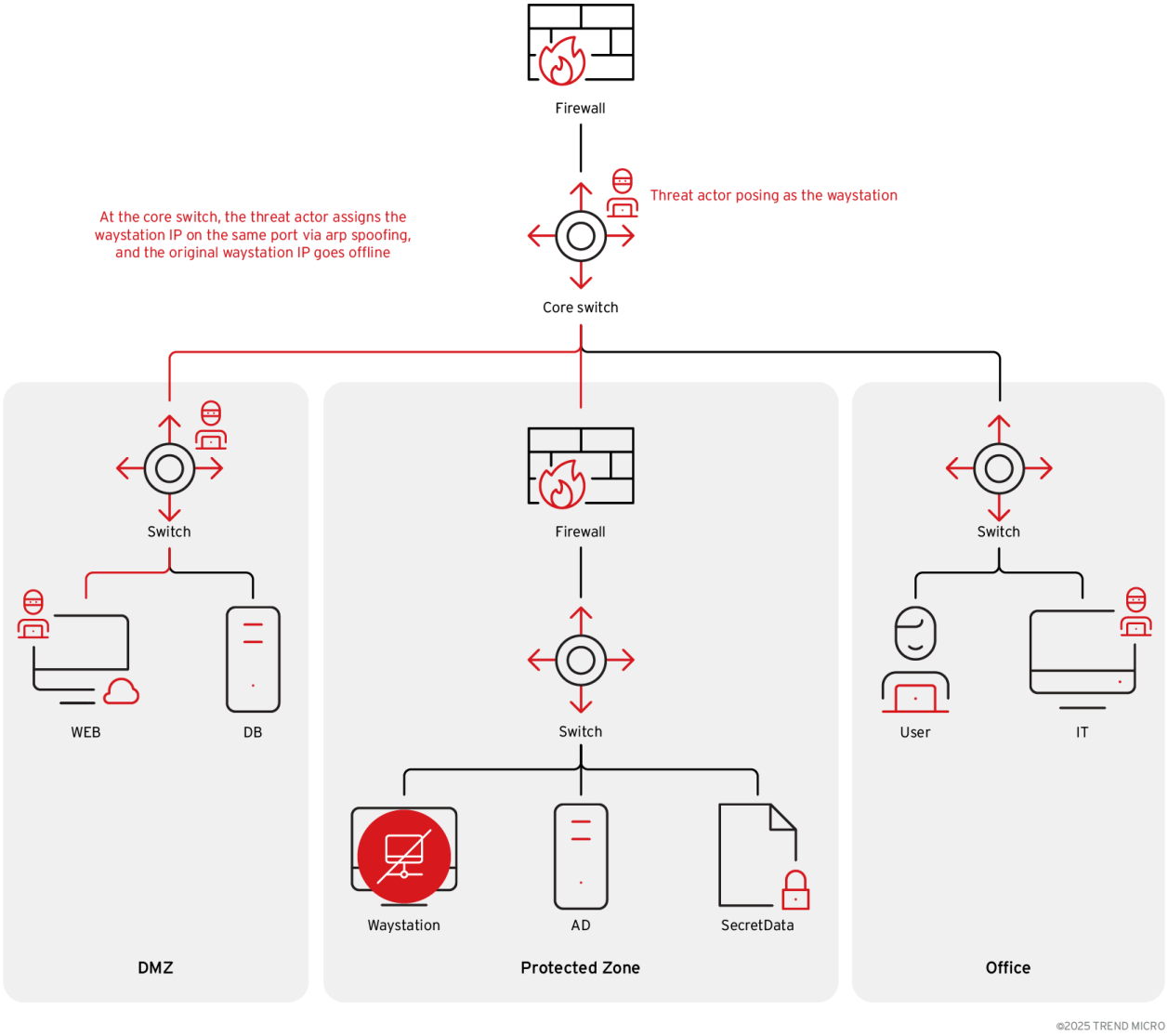

Figure 6. The attacker can gain access to other protected zones by impersonating a waystation's IP address to bypass the internal firewall.

download

The actual attacks Trend investigated are more complex, as the victims' network architectures are also more intricate.

Technical details

When the rootkit is successfully installed on the device after exploiting the vulnerabilities, the attack gains control remotely and connects different 2 VLANs, which allows for lateral movement. Trend investigation revealed the main functions of the rootkit, listed below:

- Acts as UDP listener on any port. The rootkit accepts UDP packets directed to any IP assigned to the device; notably, the port does not have to be open for this function to take effect. This channel is used by the attacker to configure or trigger backdoor functions.
- Creates a universal password (enabled by default). This functionality is implemented by modifying IOSd memory. Because it hooks low-level authentication functions, the password works across most authentication methods (AAA, local login, enable password, etc.). This change is volatile and disappears after reboot.

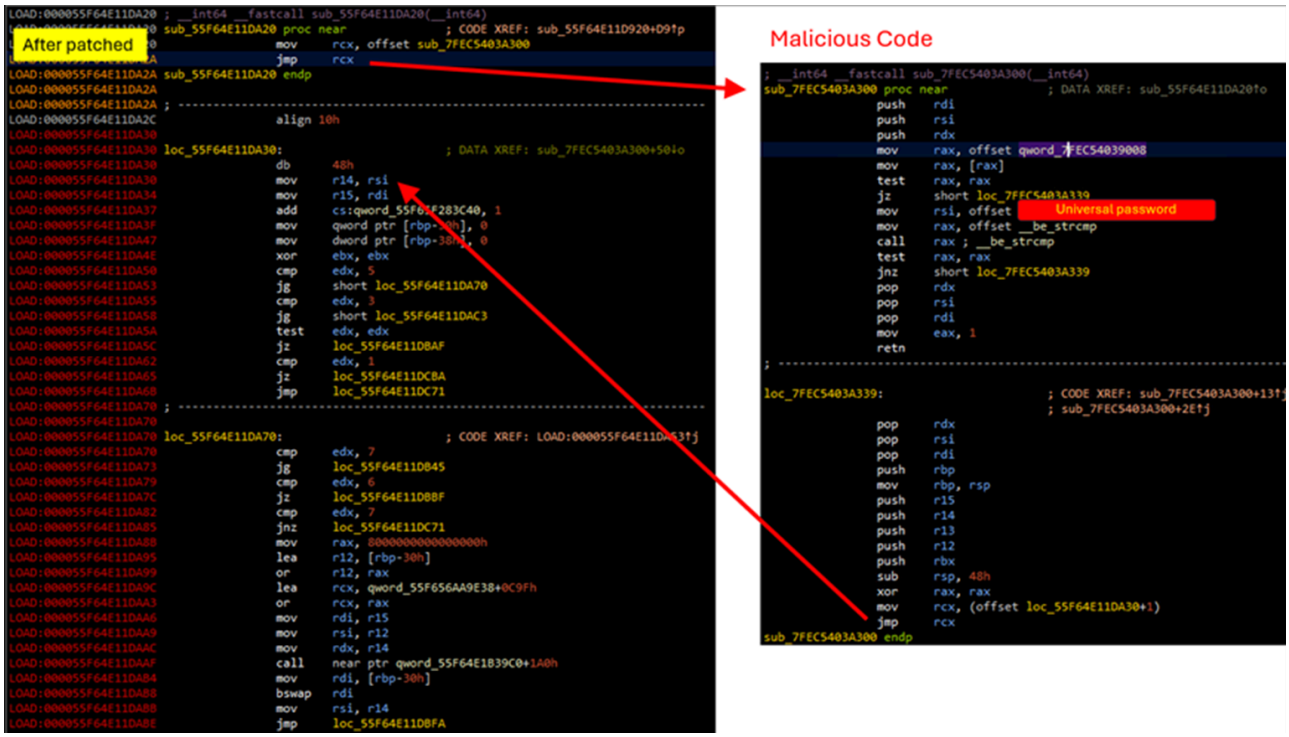

Figure 7. The modification in the IOSd memory for a universal password disappears after reboot.
download

- Hides certain running-config items in memory (disabled by default). When enabled, the rootkit hides specified account names, EEM scripts, and ACLs from the running configuration. Trend investigations revealed some hidden account names such as observed:

dg3y8dpk dg4y8epk dg5y8fpk dg6y8gpk dg7y8hpk
Hidden EEM scripts: CiscoEMX-1 to CiscoEMX-5

Hidden ACLs: EnaQWklg0, EnaQWklg1, EnaQWklg2

- Allows VTY ACL bypass (disabled by default). The cisco VTY refers to the virtual interface on a Cisco device (like a router or switch) that allows remote access via protocols such as telnet or ssh. Administrators can apply ACLs to control access to VTY lines, but if VTY is enabled, any ACL bound to it will be ignored.
- Toggles or deletes device logs. This function allows an attacker to temporarily disable log history by setting the log size to zero.
- Resets last running-config write timestamp. This is used to hide changes, so it appears the configuration was never modified.

Detection and security recommendations

Currently there is no universal automated tool that can reliably determine whether a Cisco switch has been successfully compromised by the ZeroDisco operation. If you suspect a switch is affected, we recommend contacting Cisco TAC immediately and asking the vendor to assist with a low-level investigation of firmware/ROM/boot regions.

For early detection Trend recommends utilizing Trend Cloud One™ Network Security which provides deep inspection of cloud network traffic using virtual patching, intrusion prevention (IPS), and post-compromise detection to prevent malware and zero-day attacks. It offers real-time threat intelligence, custom rule sets, behavioral analytics, and supports hybrid cloud environments, integrating with other Trend Cloud One services and Trend Vision One™ for extended detection and response (XDR).

Trend Micro™ Deep Discovery™ can also help mitigate risk by detecting the Cisco exploit and UDP controller communication. Deep Discovery uses virtual patching and intelligent threat detection to inspect inbound and outbound network traffic for advanced threats, ransomware, and targeted attacks.

Trend Cloud One Network Security and TippingPoint Threat Protection System

- 46396 - SNMP: Cisco IOS XE Software Authframework OID Get-Request Buffer Overflow Vulnerability

Deep Discovery Rules

- 5497 - UDP_CONTROLLER_REQUEST
- 5488 - SNMP_CISCO_AUTHFRAMEWORK_OID_REQUEST

Trend Vision One™ Endpoint Security Workbench

- Multiple Suspicious UDP Payload Sent Using Shell and Netcat

Proactive security with Trend Vision One™

Trend Vision One™ is the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management and security operations, delivering robust layered protection across on-premises, hybrid, and multi-cloud environments.

Trend Vision One™ Threat Intelligence

To stay ahead of evolving threats, Trend customers can access Trend Vision One™ Threat Insights which provides the latest insights from Trend ™ Research on emerging threats and threat actors.

Trend Vision One Threat Insights

- Emerging Threats: New Campaign Targets Cisco Switches with SNMP and Telnet Exploits

Trend Vision One Intelligence Reports (IOC Sweeping)

- New Campaign Targets Cisco Switches with SNMP and Telnet Exploits

Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

(ruleId: (5497 OR 5488) AND eventId:100119) OR (subRuleId: 46396 AND eventName:INTRUSION_DETECTION) AND LogType: detection

Indicators of Compromise (IoCs)

Indicators of Compromise can be found here.

With contributions from Joey Chen, Cisco TALOS Team

Tags

Latest News | Research | Exploits & Vulnerabilities | Articles, News, Reports | Cyber Threats