FORESCOUT
Active Defense for the Enterprise of Things™

AMNESIA:33 Vulnerabilities

Customer FAQ: Identify and Mitigate Risk with Forescout

Q: What is AMNESIA:33?

A: AMNESIA:33 is a set of 33 vulnerabilities impacting four open source TCP/IP stacks, which collectively serve as the foundational components of millions of connected devices around the world. The TCP/IP stacks impacted are uIP, FNET, picoTCP and Nut/Net. If exploited, these vulnerabilities could allow a cyber attacker to steal data, overload systems or even take full control of devices. AMNESIA:33 impacts more than 150 vendors and millions of IoT, OT and IT devices.

Q: Is my organization vulnerable?

A: AMNESIA:33 affects multiple open source TCP/IP stacks that are not owned by a single company. Thus, a single vulnerability tends to spread easily and quietly across multiple codebases, development teams, companies and products, presenting a significant challenge for identifying vulnerable devices. The TCP/IP stacks affected can be found in operating systems, embedded devices, systems-on-a-chip, networking equipment, OT devices and a myriad of consumer and enterprise IoT devices.

Q: How does it impact devices?

A: AMNESIA:33 affects seven different components of the stacks: DNS, IPv6, IPv4, TCP, ICMP, LLMNR and mDNS. Two vulnerabilities in AMNESIA:33 only affect 6LoWPAN wireless devices. AMNESIA:33 has four categories of potential impact, including remote code execution (RCE), denial of service (DoS via crash or infinite loop), information leak (info leak) and DNS cache poisoning. Generally, these vulnerabilities can be exploited to take full control of a target device (RCE), impair its functionality (DoS), obtain potentially sensitive information (info leak) or inject malicious DNS records to point a device to an attacker-controlled domain (DNS cache poisoning).

Q: How can I mitigate the impact of AMNESIA:33?

A: Forescout recommends six best practices to protect your organization:

- **Assess your risk.** Perform a thorough risk assessment before deploying mitigations. This includes identifying potentially vulnerable devices, their business context and criticality, and their communication pathways and internet exposure. Based on this assessment, determine what level of mitigation is required.
- **Rely on internal DNS servers.** Configure devices to rely on internal DNS servers whenever possible and closely monitor external DNS traffic, as several vulnerabilities in AMNESIA:33 are related to DNS clients, which require a malicious DNS server to reply with malicious packets.
- **Disable or block IPv6 traffic.** Since several vulnerabilities in AMNESIA:33 relate to IPv6 components, disable or block unnecessary IPv6 network traffic.

- **Segment to mitigate risk.** For unpatchable IoT and OT devices, use segmentation to minimize their network exposure and the likelihood of compromise without impacting mission-critical functions or business operations. Segmentation and zoning also limit the blast radius and business impact if a vulnerable device becomes compromised.
- **Patch when possible.** The best mitigation is to identify and patch vulnerable devices. However, this is easier said than done because:
  - Patches may not be available for an embedded component from the IoT or OT device vendor.
  - Directly patching an embedded component may void the device manufacturer's warranty.
  - A device may be part of a mission-critical function or high-availability business operation and may not be patchable until a future scheduled maintenance window.

  Patch devices when possible, and use segmentation for risk mitigation when devices can't be patched.
- **Monitor for malformed packets.** Monitor all network traffic for malformed packets (for example, having non-conforming field lengths or failing checksums) that try to exploit known vulnerabilities or possible zero days, since many vulnerabilities are related to IPv4 and other standard components of stacks. Anomalous and malformed IP traffic should be blocked, or network operators should receive alerts regarding their presence.

Q: Can Forescout help identify vulnerable devices?

A: First and foremost, use the Forescout platform for accurate identification and inventory of all devices, and identify all unknown and unauthorized devices on the network. To exploit AMNESIA:33 vulnerabilities, an attacker needs a communication path to a vulnerable device or a routed path to an internal network. Unknown and unauthorized devices may try to compromise vulnerable devices. It is paramount to use the Forescout platform to block all unauthorized devices from accessing the corporate network.

Once you have the foundational visibility, use Forescout's newly released Security Policy Template (SPT) that detects potentially vulnerable devices by flagging the characteristic network signatures of devices using uIP, Ethernut, FNET and picoTCP.

Q: I am a Forescout eyeSight customer, is there a SPT to identify vulnerable devices?

A: Yes. As mentioned above, Forescout has released a SPT that detects devices in your environment that are potentially vulnerable to AMNESIA:33. Vulnerable devices are categorized with High Certainty, Medium Certainty and Low Certainty so appropriate mitigation actions can be taken.

The SPT is now available via our customer portals:

- Flexx customers: https://forescout.force.com/support/s/downloads
- PAL customers: https://www.forescout.com/amnesia33-spt/

Q: What eyeSight techniques do I need to use to find vulnerable devices?

A: Forescout uses a combination of passive and active techniques to give you the flexibility and greater degree of certainty

in detecting vulnerable devices. These include passive techniques such as DHCP fingerprinting, HTTP parsing, TCP fingerprinting, compromised device vendor look up and active techniques such as NMAP and ICMP scans. Whilst not all techniques need to be enabled, multiple vectors of assurance provide a higher degree of confidence.

For sensitive environments, such as OT and medical IoTs, passive-only techniques can be used. For smaller remote sites that often cannot provide SPAN traffic, other passive and active techniques are available for full visibility into vulnerable and potentially vulnerable devices across all parts of the network.

Q: Can Forescout help mitigate the risk from vulnerable devices?

A: Yes. Forescout can help in multiple ways to reduce the risk associated with AMNESIA:33 vulnerabilities. Following defense in-depth principles, it is advisable to adhere to as many of these risk mitigation best practices as is feasible.

- **Patch when possible.** For devices with available patches and that can be patched outside of maintenance windows, the Forescout platform can help orchestrate remediation workflows with other IT and security tools.
- **Segment to mitigate risk.** Devices connected directly to the internet are at the greatest risk for AMNESIA:33 vulnerabilities. Forescout's platform provides a network flow mapping of existing communications, which is not just a prerequisite for designing effective segmentation zones. It also provides a baseline understanding of external and internet-facing communication paths. This can help identify unintended/anomalous external communications allowing enforcement of appropriate segmentation controls for mitigating risk. Upon identifying vulnerable devices, logically group those assets to form the basis for segmentation-based mitigation. It's important to consider the business function of the asset while logically grouping devices, as the mitigation actions on a printer may be different than a business-critical IoT device. At that point, customers can detect and block anomalous IP traffic and apply segmentation controls to decrease the communication allowed to/from these potentially vulnerable devices, thereby limiting the likelihood of compromise and the blast radius if a compromise occurs.
- **Enforce security compliance.** Use the Forescout platform to continuously monitor and enforce security compliance for all connected Enterprise of Things devices. Noncompliant devices (e.g., unpatched devices or those with weak/default credentials and legacy OSes, among others) are often the primary targets for attackers.
- **Monitor network communications.** In addition to immediately reducing risk by taking mitigation actions, customers should continuously monitor the traffic to and from these high-risk devices. The Forescout platform monitors the ongoing traffic and behavior of the device, so when anomalous traffic flows are detected, response actions or more stringent controls can be enforced.

Q: I am a Forescout eyeInspect (formerly SilentDefense™) customer. Can I detect AMNESIA:33 vulnerabilities on my OT network?

A: Yes. Forescout has released two eyeInspect scripts that detect active exploitation of AMNESIA:33 vulnerabilities, so critical alerts/mitigation steps can occur upon detection of an active attack. Please contact your Forescout representative or SE to obtain those scripts.

Additional Resources

- What is AMNESIA:33 video
- AMNESIA:33 Research Report
- AMNESIA:33 Research Report Executive Summary
- AMNESIA:33 Vulnerabilities On-Demand Webinar
- AMNESIA:33 White Paper
- Forescout Research Labs AMNESIA:33 Blog
- Step-by-step video using Forescout Security Policy Templates

forescout.com/amnesia33/   research@forescout.com   toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (U.S.) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com