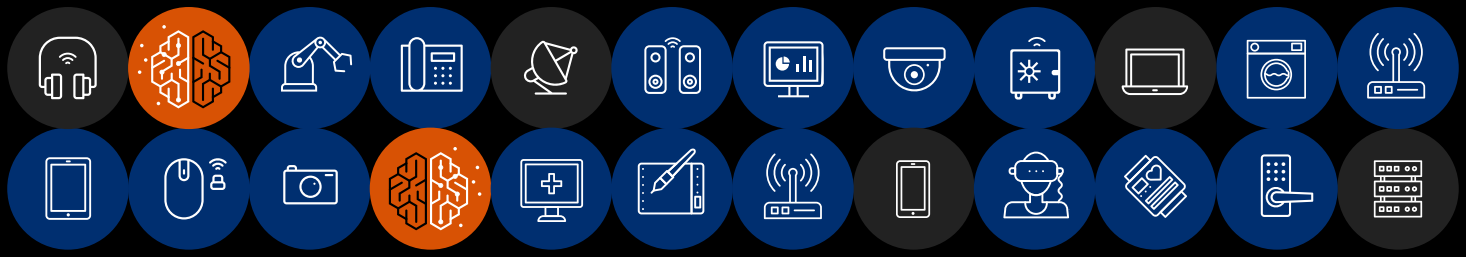
FORESCOUT
Active Defense for the Enterprise of Things™

AMNESIA:33

Research Report Executive Summary



- Forescout Research Labs has launched Project Memoria, **an initiative** that aims at providing the community with the **largest study on the security of TCP/IP stacks**. Project Memoria's goal is to develop the understanding of common bugs behind the vulnerabilities in TCP/IP stacks, identifying the threats they pose to the extended enterprise and how to mitigate those.
- **AMNESIA:33** is the first study we have published under Project Memoria. In this study, we discuss the results of the security analysis of seven **open source TCP/IP stacks** and report a bundle of **33 new vulnerabilities** found in four of the seven analyzed stacks that are used by major IoT, OT and IT device vendors.
- **Four of the vulnerabilities in AMNESIA:33 are critical**, with potential for remote code execution on certain devices. Exploiting these vulnerabilities could allow an attacker to take control of a device, thus using it as an entry point on a network for internet-connected devices, as a pivot point for lateral movement, as a persistence point on the target network or as the final target of an attack. For enterprise organizations, this means they are at increased risk of having their network compromised or having malicious actors undermine their business continuity. For consumers, this means that their IoT devices may be used as part of large attack campaigns, such as botnets, without them being aware.

150+

VENDORS AFFECTED

- AMNESIA:33 affects **multiple open source TCP/IP stacks** that are **not owned by a single company**. This means that a single vulnerability tends to **spread easily and silently** across multiple codebases, development teams, companies and products, which presents significant challenges to patch management.
- We estimate that more than 150 vendors and millions of devices are vulnerable to AMNESIA:33. However, **it is difficult to assess the full impact** of AMNESIA:33 because the vulnerable stacks are widely spread (across different IoT, OT and IT devices in different verticals), highly modular (with components, features and settings being present in various combinations and code bases often being forked) and incorporated in undocumented, deeply embedded subsystems. For the same reasons, these vulnerabilities tend to be very hard to eradicate.
- The TCP/IP stacks affected by AMNESIA:33 can be found in operating systems for embedded devices, systems-on-a-chip, networking equipment, OT devices and a myriad of enterprise and consumer IoT devices.
- TCP/IP stacks are critical components of all IP-connected devices, including IoT and OT, since they enable basic network communication. A security flaw in a TCP/IP stack can be extremely dangerous because the code in these components may be used **to process *every* incoming network packet that reaches a device**. This means that some vulnerabilities in a TCP/IP stack allow for a device to be exploited even when it simply sits on a network without running a specific application.
- Many of the vulnerabilities reported within **AMNESIA:33** arise from bad software development practices, such as an absence of basic input validation. They relate mostly to **memory corruption** and can cause **denial of service, information leaks** or **remote code execution**.
- Due to the complexity of identifying and patching vulnerable devices, vulnerability management for TCP/IP stacks is becoming a challenge for the security community. We recommend **adopting solutions that provide granular device visibility**, allow the monitoring of network communications and isolate vulnerable devices or network segments to manage the risk posed by these vulnerabilities.

Don't just see it. Secure it.™

Contact us today to actively defend your Enterprise of Things.

Download the full report: Learn the details of our research and what mitigation techniques can be put in place.

Download the white paper: Discover how Forescout helps you actively defend against AMNESIA:33, including six best practices to protect your organization.

View the webinar: Listen to our experts describing the highlights of the research.

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