FORESCOUT
Active Defense for the Enterprise of Things™

AMNESIA:33

Identify and Mitigate the Risk From Vulnerabilities Lurking in Millions of IoT, OT and IT Devices

33 Zero-Day Vulnerabilities in Four Widely Used Open Source TCP/IP Stacks

Forescout Research Labs has discovered 33 zero-day vulnerabilities impacting four widely used open source TCP/IP stacks. Dubbed AMNESIA:33, these vulnerabilities reside in the uIP, FNET, picoTCP and Nut/Net stacks, which serve as foundational connectivity components for millions of IoT, OT, networking and IT devices. Four of these vulnerabilities are **critical and allow for remote code execution**.

Primarily, these vulnerabilities cause **memory corruption** and can be exploited for:

- Remote code execution (RCE) to take control of a target device
- Denial of service (DoS) to impair functionality and impact business operations
- Information leak (Infoleak) to acquire potentially sensitive information
- DNS cache poisoning to point a device to a malicious website

4
CRITICAL VULNERABILITIES

150+
VENDORS AFFECTED

1M+
DEVICES VULNERABLE

These vulnerabilities affect multiple components of the four TCP/IP stacks, including DNS, IPv6, IPv4, TCP, ICMP, LLMNR and mDNS.

While it is difficult to assess the full impact of AMNESIA:33, we estimate more than **150 vendors and millions of devices** worldwide are vulnerable. Since these open source stacks are widely used in embedded components, they exist in devices used in most modern enterprises. Affected devices range from network switches to smart printers, environmental sensors to security cameras, self-checkout kiosks to RFID asset trackers, and badge/fob readers to uninterruptible power supplies, to name just a few.

Forescout Research Labs discovered the AMNESIA:33 vulnerabilities as part of Project Memoria, an initiative that aims at providing the cybersecurity community with the largest study on the security of TCP/IP stacks. Forescout Device Cloud, a data lake of over 12 million enterprise devices, was leveraged to identify potentially vulnerable devices and determine the impact on IoT, OT and IT devices commonly used in the modern enterprise.

The Far-Reaching Impact of AMNESIA:33

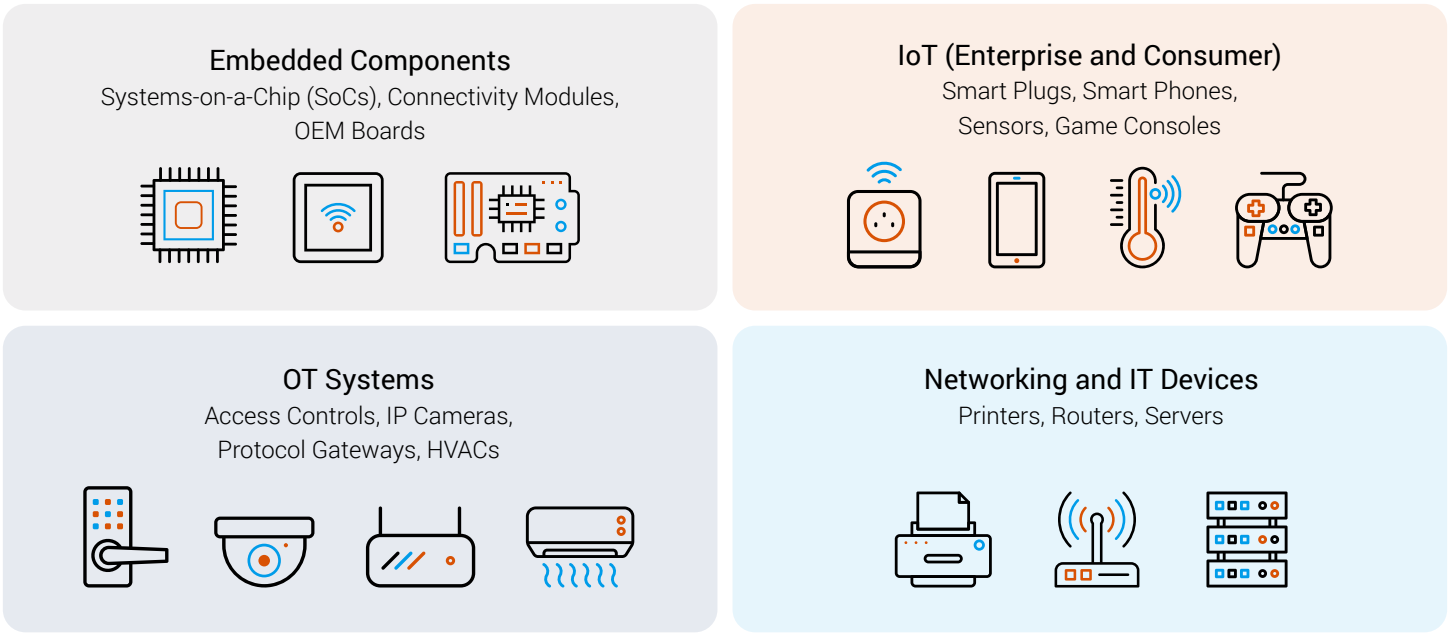
The widespread nature of these vulnerabilities means that countless organizations around the world could be at risk. What makes AMNESIA:33 so pervasive and far-reaching?

- TCP/IP stacks are **foundational components** of all IP-connected devices, including IoT and OT, since they enable basic network communication. Code in these stacks processes every incoming network packet that reaches a device, allowing vulnerabilities to be exploited even when a device simply sits on the network without running specific applications or listening on a particular port. A security flaw in a TCP/IP stack can be extremely dangerous because a single network packet can be used to control or crash a device.
- Open source software is commonly used in embedded components and IoT/OT devices. Tesla, Siemens, Honeywell and most other advanced technology companies leverage open source software. Since **source code is re-used in** [88% of embedded projects], it acts as a force multiplier for vulnerabilities such as AMNESIA:33 that

> **Over 80% of organizations currently use IoT to solve business use cases, and almost 20% of organizations have already detected an IoT-based attack in the past three years.[1]**
>
> **GARTNER**
> **JANUARY 2020**

are found in embedded components. Of these embedded projects, 58% use an open source RTOS (Real-time Operating System), which typically includes an open source embedded TCP/IP stack.

- Unlike other recent TCP/IP stack vulnerabilities such as Ripple20, 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 silently across multiple codebases, development teams, companies and products, presenting significant challenges to vulnerability and patch management.
- It is rare to have a complete list of all hardware and software components, known as a Bill of Materials (BOM), for IoT and OT devices. These components come from a device vendor's supply chain, and may run embedded software such as TCP/IP stacks. The numbers and types of embedded components in devices often come as a surprise to the end user, and the same can often be said for device vendors. Thus, there is no way to know precisely how many devices are affected by AMNESIA:33, and actual device numbers may **far exceed current estimates** of millions of vulnerable devices in enterprise networks.



Examples of components and devices running the vulnerable stacks

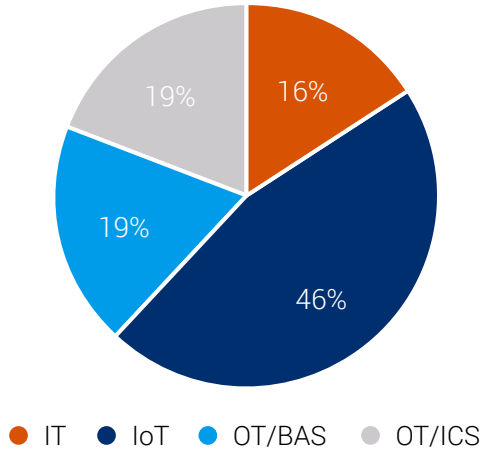
To determine the reach of AMNESIA:33, we leveraged the Forescout Device Cloud, a data lake of over 12 million devices from some of the largest and most heavily targeted enterprises in the world. Researchers also leveraged open source documentation and tools, such as Shodan and Censys, to identify the use of these TCP/IP stacks. Our analysis indicates potential impact across millions of IoT, OT and IT devices used in the modern enterprise:

- **IoT devices** (both enterprise and consumer), such as cameras, environmental sensors (e.g., temperature, humidity), smart lights, smart plugs, barcode readers, specialized printers and audio systems for retail
- **Building Automation Systems**, such as physical access control, fire and smoke alarms, energy meters and HVAC systems
- **OT equipment for Industrial Control Systems**, such as RTUs, protocol gateways and serial-to-ethernet gateways
- **Networking equipment and IT devices** such as printers, switches and wireless access points

Forescout Device Cloud and online instances of devices also revealed the potential impact across a wide swath of industries, with government, healthcare, services and manufacturing having the highest potential exposure.

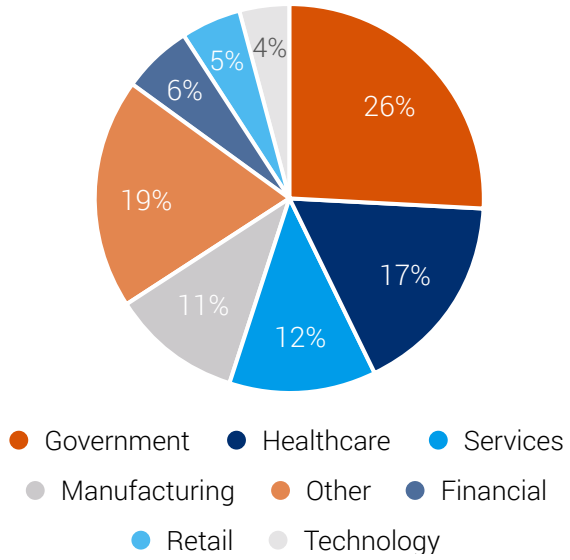
The widespread nature of these vulnerabilities means that many organizations around the world may be affected by AMNESIA:33. Organizations that fail to mitigate this risk are leaving the door open for attackers to exploit IoT, OT and IT devices across their organization.

% of Vulnerable Devices per Type



Potentially vulnerable devices by type

% of Vulnerable Devices per Industry



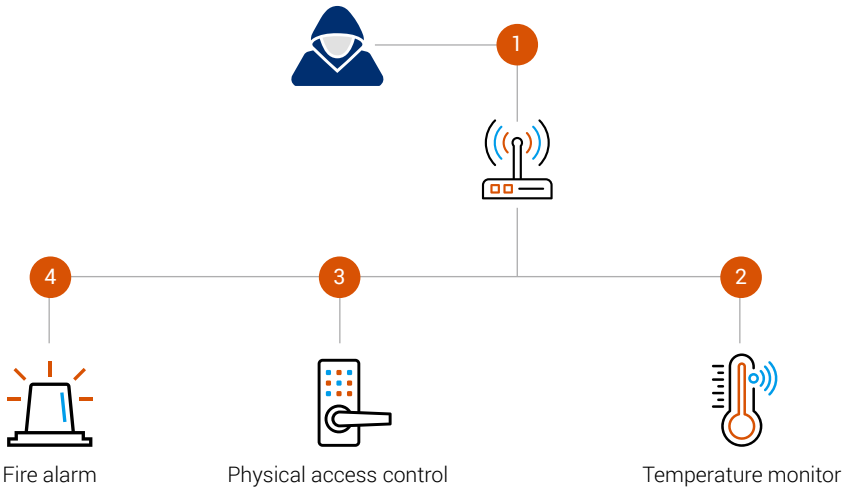
Potentially vulnerable devices by industry

The Risks and Attack Scenarios

Exploiting the AMNESIA:33 vulnerabilities could allow an attacker to take control of a device, thus using it as:

- An **entry** point on a network
- A **pivot** point for lateral movement
- A **persistence** point on the target network
- The **final target** of an attack

For enterprise organizations, this means they are at increased risk of having their networks compromised or having malicious actors undermine their business continuity. For consumers, this means that their IoT devices may be used as part of large-scale attack campaigns, such as botnets, without them being aware. Here are some industry-specific attack scenarios:

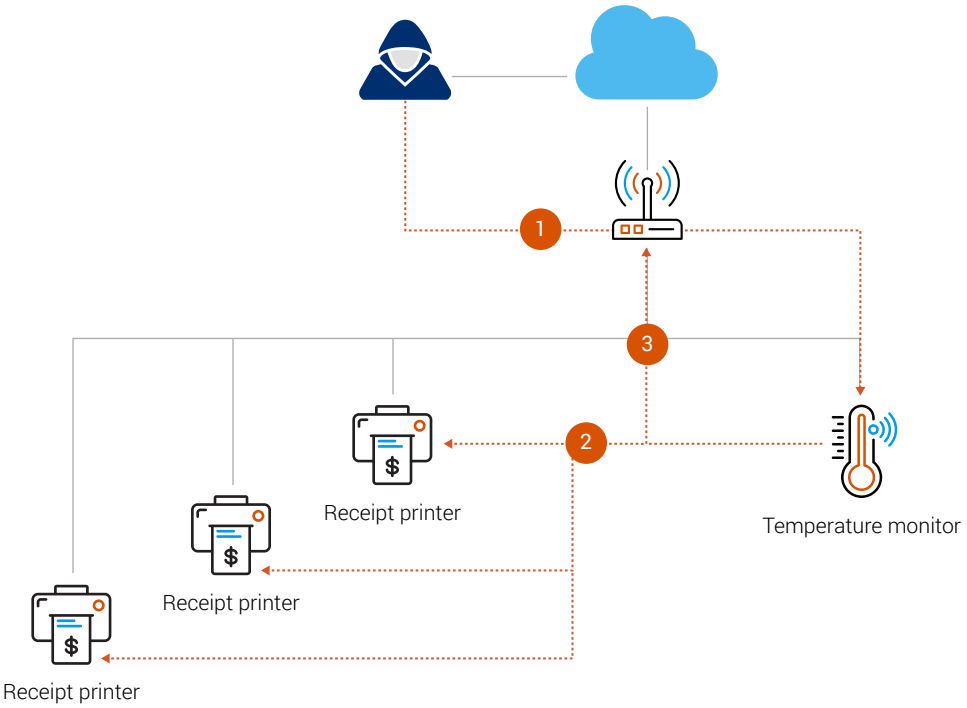


AMNESIA:33 attack scenario in Healthcare

Healthcare:

The attacker's goal is to create chaos in a hospital by disrupting IoT devices.

1. **Initial access:** An attacker obtains access to the network by physically being present at a hospital and connecting to an exposed Ethernet socket in a patient's room. By leveraging the flawed network segmentation in healthcare networks, the attacker can access several devices to disrupt their normal functioning.
2. **Impact 1:** The attacker can disable a temperature monitor in a storage room to spoil medications or patient samples.
3. **Impact 2:** The attacker can tamper with physical access control systems to access restricted areas or lock people within those areas.
4. **Impact 3:** The attacker can disable fire alarm systems to open the way for physical attacks that jeopardize the safety of patients and employees.

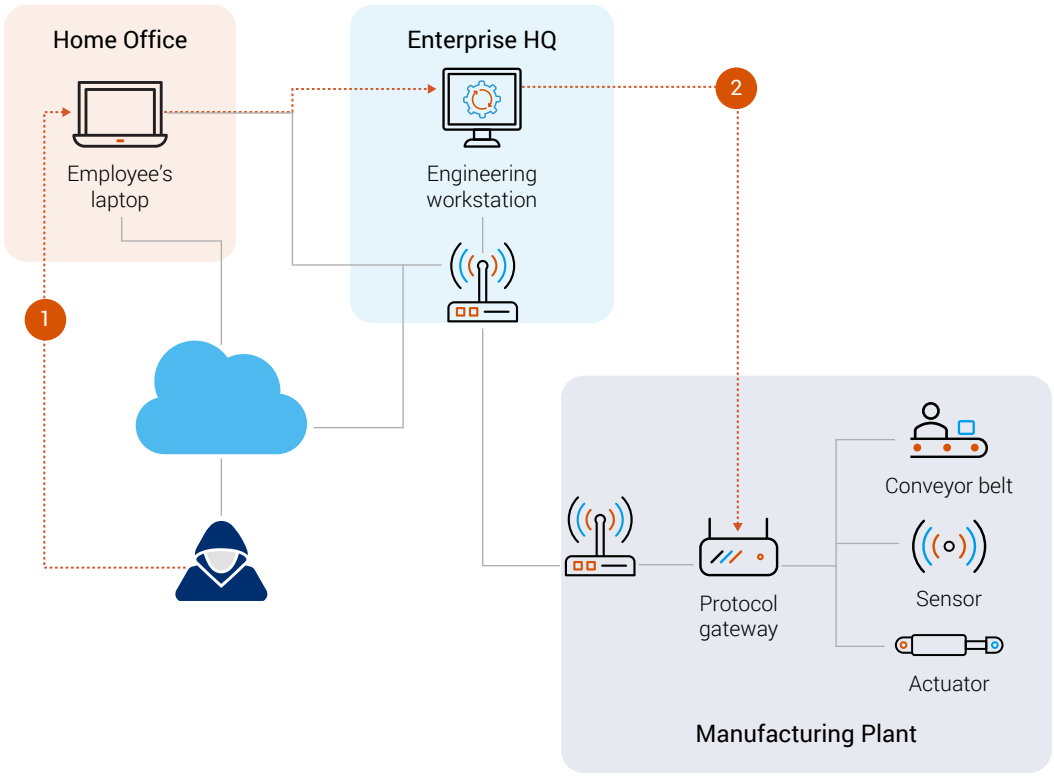


AMNESIA:33 attack scenario in Retail

Retail:

The attacker's goal is to sabotage a retail shop during a busy period, using an IoT device as an entry point.

1. **Initial access:** An attacker exploits a temperature monitor (which we often see connected to the internet) to gain a foothold on a shop's network.
2. **Impact 1:** Once inside the network, the attacker can leverage the temperature monitor to send malicious packets that take several receipt printers for the Point-of-Sale (PoS) systems offline, causing massive delays during the busy holiday shopping season.
3. **Impact 2:** To further impact the retailer, the attacker can also target the network switch, thus disabling communication between the shop's network and its corporate services.



AMNESIA:33 attack scenario in Manufacturing

Manufacturing:

The attacker's goal is to tamper with a production line via its OT network.

1. **Initial access and lateral movement:** The attacker first compromises a VPN connected to a remote employee's laptop via a phishing attack. After compromising the laptop, the attacker moves laterally by exploiting EternalBlue, ZeroLogon or another Windows vulnerability to an engineering workstation that manages a manufacturing plant production line. From there, the attacker can finally reach critical devices at the plant.
2. **Impact:** The attacker chooses to tamper with a protocol gateway that connects serial-enabled physical equipment in a production line (such as conveyor belts, sensors and actuators) to the control network. This allows the attacker to halt production, disable quality control, or inject false data to create products that are not up to the company's standards.

Mitigating the Risk: The Patching Challenge

While IoT and OT devices bring undeniable benefits to the modern enterprise in terms of automation, efficiency and powering new services, they present unique challenges for vulnerability and patch management.

Given the widespread use of open source and embedded components in IoT and OT devices, it is rare to have a complete software bill of material (BoM). The **long and fuzzy nature of the supply chain** may not be evident at first glance. For example, a Broadlink Smart Plug uses a system-on-a-chip (SoC), which contains the popular MediaTek MT7681 Wi-Fi module, which leverages the vulnerable uIP stack. Hence, it may not be evident that the Broadlink Smart Plug is vulnerable to AMNESIA:33 and requires patching.

Supply chain example, the Broadlink Smart Plug

Even if the supply chain is well understood, patch management may be a challenge because of a **broken link in the supply chain**. In this real-world example (anonymized due to the critical nature of the assets involved), vendor D of UPS devices relies on vendor C for network management cards, which integrates an embedded RTOS from vendor B that includes the vulnerable TCP/IP stack from vendor A. As is the case in this real-world example, vendor B of the RTOS is no longer in business, and even if the uIP stack from vendor A is patched, this patch will not become part of the RTOS distribution or the network management card, leaving the UPS un-patchable.

Supply chain example, security issues on a UPS

This is a far cry from traditional IT devices where device and software vendors actively manage their supply chain and provide patches for all components. Even the customer effort for patching is easier because software components can generally be patched independently of firmware, user devices can be patched frequently, and application servers have well-defined and frequent maintenance windows.

The patch management challenge for IoT and OT devices is multi-faceted:

- Patches may not be available for embedded components from device vendors, as in the example above
- Directly patching embedded components may void a device manufacturer's warranty
- Critical infrastructure and high-availability business operations may not allow patching devices until scheduled and infrequent maintenance windows

Due to the complexity of identifying and patching vulnerable devices, organizations need to look beyond patching for risk mitigation best practices as described in the next section.

Best Practices for Risk Mitigation

Due to the high effort involved in identifying and patching all vulnerable devices, organizations should consider a wider spectrum of mitigating and compensating controls.

Risk mitigation best practices include:

- ***Assess your risk and exposure:*** Organizations should perform a risk assessment before deploying mitigations. This includes identifying potentially vulnerable devices, their business context and criticality and their communications pathways and internet exposure. Use solutions that provide network-based device visibility; granular classification and identification of IoT, OT and IT devices; and network communications monitoring. 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 are related to IPv6 components, disable or block unnecessary IPv6 network traffic.
- ***Segment to mitigate risk:*** For IoT and OT devices that cannot be patched, 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 embedded components from the IoT or OT device vendor
  - Directly patching embedded components 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 scheduled maintenance window at a future time
- ***Monitor for malformed packets:*** Monitor all network traffic for malformed packets (for instance, 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 its presence should at least be monitored by network operators.

How Forescout Can Help

While there is no silver bullet to completely eliminate your risk and exposure to AMNESIA:33, Forescout can help in several ways to identify and mitigate your risk.

The Forescout product set of eyeSight, eyeInspect, eyeControl, eyeSegment and eyeExtend provides existing capabilities, as well as newly released detection templates and scripts that can be used to:

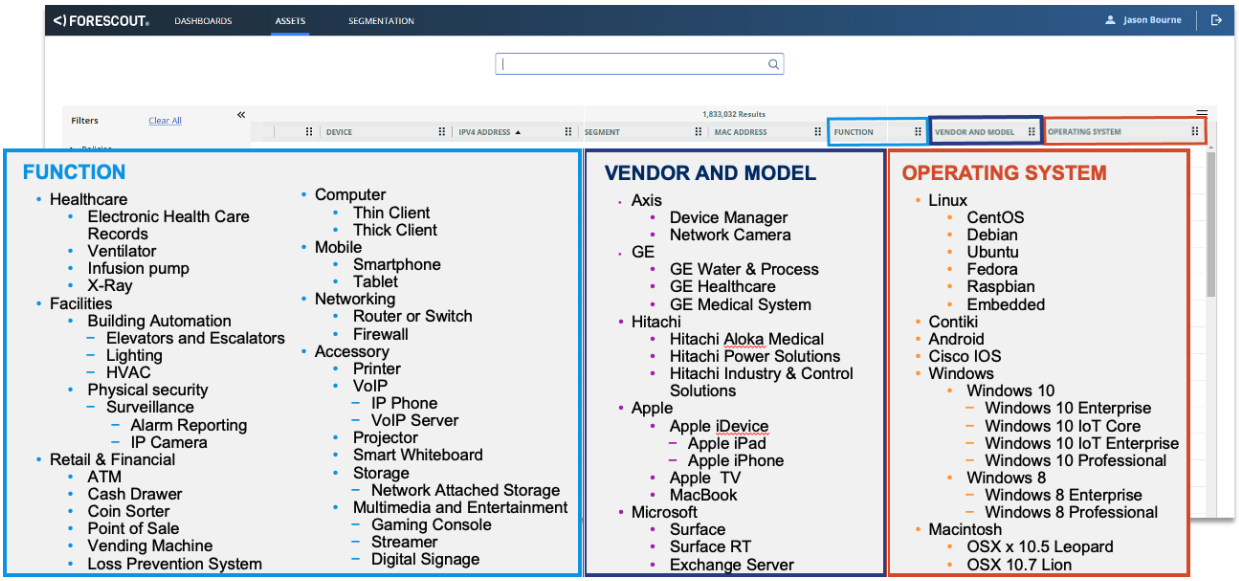
- Get an **accurate real-time inventory** of all IoT, OT and IT devices connected to your network
- Detect and potentially **block unknown, unauthorized and spoofing** devices on your network to lower your risk of exploitation
- Identify **vulnerable and potentially vulnerable devices** using the newly released eyeSight Security Policy Template (SPT)
- Identify potential **exploitation of AMNESIA:33 vulnerabilities** in OT environments using the newly released eyeInspect SD script
- For devices that can be patched, **orchestrate remediation workflows** with the Forescout solution and other IT/security tools
- For vulnerable and potentially vulnerable devices that cannot be patched, **apply segmentation policies** as a compensation control to reduce risk using eyeSegment
- Monitor traffic to and from high-risk devices and enforce more stringent controls using eyeControl if **anomalous traffic or malformed packets** are detected

Know what is on your network

Accurate identification and inventory of all devices are foundational for risk assessment and mitigation. Use eyeSight and eyeInspect to get a three-dimensional view (Device Function and Type, Vendor and Model, OS and Version) of all IoT, OT and IT network-connected devices, and identify any unknown, unauthorized or spoofing devices on the network.

Forescout provides a choice of more than 20 configurable active and passive techniques to discover and classify all types of devices connecting anywhere on your network. This gives you the most comprehensive agentless visibility via deep integration with existing IT and OT network infrastructure without requiring network upgrades or changes. It eliminates your blind spots and gives you rich context about connected devices, including their identity, state, configuration, posture and where and how they are connecting to 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, unauthorized or spoofing devices may try to compromise vulnerable devices. It is paramount that you identify and block all unauthorized devices from accessing the corporate network.



Real-time identification and three-dimensional classification of connected devices

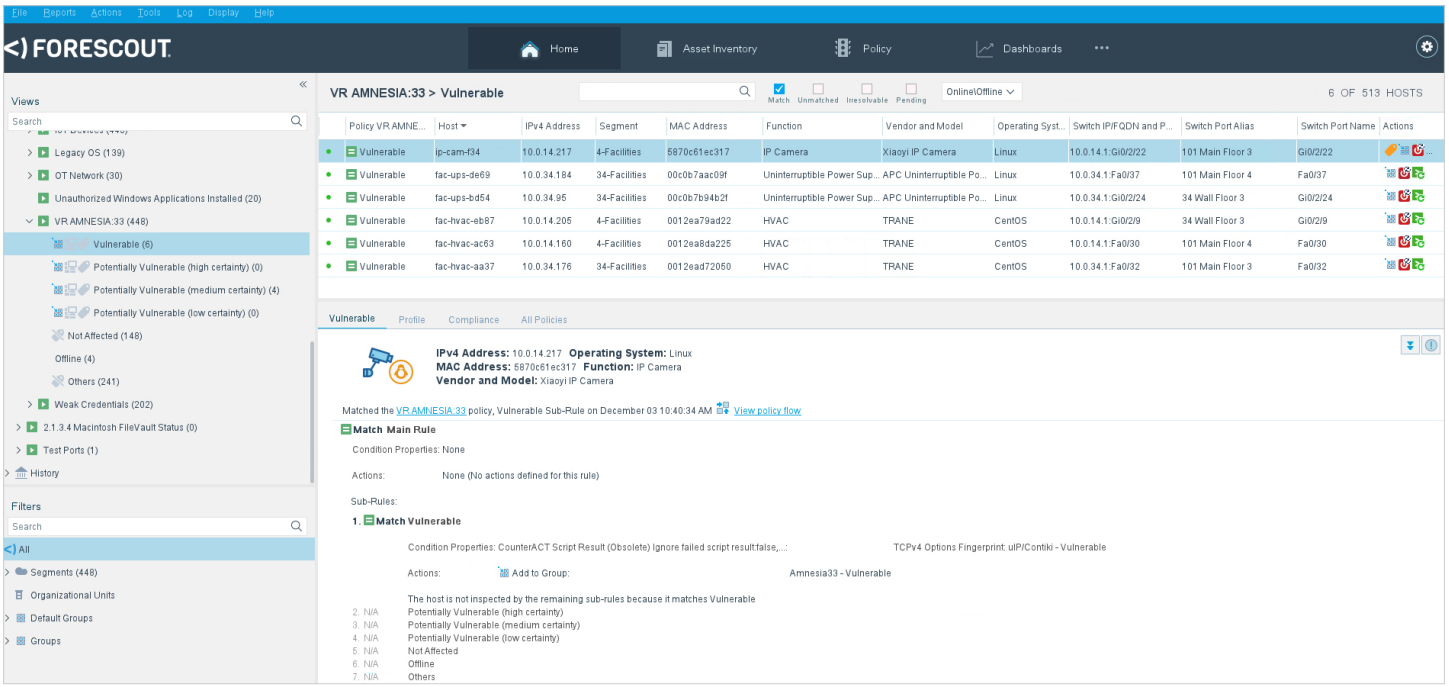
Identify potentially vulnerable devices to assess your risk

Once you have the foundational visibility, use the newly released eyeSight Security Policy Template (SPT) to detect vulnerable and potentially vulnerable devices. The SPT identifies devices running the vulnerable stacks by detecting the characteristic network signatures of the uIP, FNET, picoTCP and Nut/Net stacks.

Policies you create with this template use passive and active techniques, such as HTTP parsing (via Active Inspection or SPAN), DHCP fingerprinting (via IP-helper or SPAN), TCP fingerprinting (via Active Inspection or SPAN), device vendor/model lookup, NMAP and ICMP probing, to detect vulnerable and potentially vulnerable devices.

For environments with sensitive devices, such as Internet of Medical Things (IoMT) or OT/ICS, 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.

For OT environments, you can also use the newly released eyeInspect SD script, which detects active exploitation of these vulnerabilities.



Identifying devices vulnerable to AMNESIA:33

Patch vulnerable devices if possible

Once you've identified vulnerable and potentially vulnerable devices, you can group them in eyeSight by device type, vendor, model, patch availability etc., to assist with mitigation steps.

For devices that have available patches and that can be patched immediately (outside of future scheduled maintenance windows), Forescout can help orchestrate remediation workflows with other IT and security tools. Devices can be temporarily isolated/quarantined in remediation VLANs using eyeControl to assist with patch management.

Vendor-provided patch management tools or IoT lifecycle management and remediation tools such as Phosphorus can be triggered to complete the patching process before provisioning regular network access to the vulnerable device.

Segment vulnerable devices to mitigate risk

Use segmentation as a compensating control to mitigate risk for vulnerable or potentially vulnerable devices that cannot be patched.

Devices directly connected to the internet are at most risk from AMNESIA:33. eyeSegment provides network flow mapping of existing communications for a baseline understanding of external and internet-facing communication paths. This can help identify unintended and anomalous external communications so appropriate network controls can be enforced with eyeControl for mitigating risk.

Once vulnerable and potentially vulnerable devices have been identified, logically group them into zones to form the basis for risk-based segmentation. When creating these zones, consider the business function of each device, as you might want to utilize different mitigation actions based on these differences (e.g., mitigation actions on a printer may be different from a business-critical IoT device).

Apply segmentation controls to decrease the communication allowed to and from vulnerable and potentially vulnerable devices. This will reduce the likelihood of compromise (limit your exposure) and the blast radius if a device is compromised (limit the impact). Forescout eyeSegment allows you to run your segmentation policies in simulation and alerting mode if you don't want to proactively enforce policies or automate enforcement using eyeControl.

Actively Defend Against AMNESIA:33

Organizations should actively identify and mitigate the risk associated with AMNESIA:33 vulnerabilities. While there is no silver bullet to defend against potential exploits, Forescout can help mitigate the risk and implement compensating controls.

Visit the Forescout website. Learn more about AMNESIA:33, including additional resources to help you understand these vulnerabilities and take action to mitigate risks.

Read the customer FAQ. Learn more about how the eyeSight SPT helps with vulnerability detection and the eyeInspect SD Script automates exploit detection.

Request a demo: Visit the Forescout demo page to request a personal demo and access a full complement of on-demand demos and video options.

Read the Forescout research report: Learn more about how Forescout Research Labs is at the forefront of IoT and OT security research and details about the AMNESIA:33 vulnerabilities.

1. Gartner – IoT Security Primer: Challenges and Emerging Practices, 6 January 2020

Don't just see it.
Secure it.™

Contact us today to actively defend your Enterprise of Things.

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