FORESCOUT

NUCLEUS:13 – Nucleus TCP/IP Vulnerability Research Disclosure

Q: What is NUCLEUS:13?

A: Forescout Research Labs and Medigate disclosed a set of 13 new vulnerabilities affecting the Nucleus TCP/IP stack, owned by Siemens.

The nature of these vulnerabilities could lead to heightened risk and expose healthcare organizations as well as others in verticals such as government, retail, financial services, and manufacturing, according to data from the Forescout Device Cloud.

NUCLEUS:13 further illustrates the problems with TCP/IP stacks that we have seen before in Project Memoria.

Q: What devices run Nucleus?

A: Nucleus is used by several devices with safety and security requirements such as medical devices and industrial systems. On Device Cloud, we see evidence of several building automation controllers from major vendors using the stack. We also see industrial controllers, VoIP phones, anesthesia machines, patient monitors, and ultrasound machines. The most affected verticals are healthcare, government, and retail.

Q: What is the impact of the vulnerabilities?

A: Understanding where the vulnerable code is present is notoriously challenging. We try to estimate the impact of NUCLEUS:13 based on the evidence collected during our research, using three main sources:

- The official Nucleus website, according to which the RTOS is deployed in more than 3 billion devices. A quick look at the page listing customer success stories reveals its use in scenarios such as healthcare (ZOLL defibrillators and ZONARE ultrasound machines), IT (BDT AG storage systems) and critical systems (Garmin avionics navigation). But we believe that most of those 3 billion are actually device components such as MediaTek IoT chipsets and baseband processors used in smartphones and other wireless devices. We also found technical documentation detailing the use of Nucleus for medical devices.
- Shodan Queries. Shodan is a search engine that allows users to look for devices connected to the Internet. We queried Shodan, looking for devices showing some evidence (e.g., application-layer banners) indicating the use of Nucleus. With a query executed on 05/Aug/2021, we found more than 2,200 instances of devices running the Nucleus FTP server ("220 Nucleus FTP") or the RTOS ("Operating System: Nucleus PLUS").
- Forescout Device Cloud. Forescout Device Cloud is a repository of information of 13+ million devices monitored by Forescout appliances. We queried it for similar banners as Shodan, as well as other information, based on DHCP signatures, for instance. We found close to 5500 devices from 16 vendors in 127 customers. Thirteen of these customers had more than 100 vulnerable devices with healthcare being the most impacted sector.

Q: Where can I find the full NUCLEUS:13 report?

A: Here

Q: How are affected vendors being notified?

A: Forescout's intent is to collaborate with affected vendors in a transparent manner and help them to identify impacted products and prepare advisories. This proven responsible disclosure process ensures all community stakeholders have the most complete information and time to prepare to take action on mitigation steps.

Q: What can organizations do to mitigate the risk from these vulnerabilities?

A: Complete protection against NUCLEUS:13 requires patching devices running the vulnerable versions of Nucleus. Siemens has released its official patches and device vendors using this software should provide their own updates to customers. Below, we discuss mitigation strategies for network operators.

Given that patching embedded devices is notoriously difficult due to their mission-critical nature, we recommend the following mitigation strategy:

- **Discover and inventory devices running Nucleus.** Forescout Research Labs has released an open-source script that uses active fingerprinting to detect devices running Nucleus. The script is updated constantly with new signatures to follow the latest development of our research. **Forescout has also released an updated Security Policy Template (SPT) for eyeSight and an updated HLI Addons script for eyeInspect to detect devices running the stack.**
- **Enforce segmentation controls and proper network hygiene** to mitigate the risk from vulnerable devices. Restrict external communication paths and isolate or contain vulnerable devices in zones as a mitigating control if they cannot be patched or until they can be patched.
- **Monitor progressive patches released by affected device vendors** and devise a remediation plan for your vulnerable asset inventory, balancing business risk, and business continuity requirements.
- **Monitor all network traffic for malicious packets** that try to exploit known vulnerabilities or possible 0-days. Anomalous and malformed traffic should be blocked, or at least alert its presence to network operators. **Forescout has released a script for eyeInspect that detects exploitation attempts against the vulnerabilities in NUCLEUS:13.**

Q: What should I do if a Forescout customer wants to speak with us about the vulnerabilities?

A: Forescout Research Labs are available to speak with vendors and asset owners that are affected by these vulnerabilities. To set up a call, send an email to research@forescout.com.

Q: Where do I go for more information?

A: For more information on the vulnerabilities and mitigation strategies, reference our external blog.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA
Intl. +1.408.213.3191
Support +1.708.237.6591