FORESCOUT

INFRA:HALT NicheStack TCP/IP

Vulnerability Research Disclosure

Q: What is INFRA:HALT?

A: Forescout Research Labs and JFrog Security Research disclosed a set of 14 new vulnerabilities affecting the NicheStack TCP/IP stack, originally developed by InterNiche Technologies and acquired by HCC Embedded in 2016.

The nature of these vulnerabilities could lead to heightened risk and expose national critical infrastructure at a time when the industry is seeing an increase in OT attacks against global utilities, oil and gas pipeline operators as well as healthcare and the supply chain.

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

Q: What devices run NicheStack?

A: NicheStack is used by several devices in the Operational Technology (OT) space, such as Siemens products. Other major OT device vendors, such as Emerson, Honeywell, Mitsubishi Electric, Rockwell Automation, and Schneider Electric have deployed the stack in their solutions. **The most affected OT verticals are Process and Discrete Manufacturing.**

The stack has been around for a while (two decades) and was distributed in several "flavors" by OEMs such as STMicroelectronics, Freescale (NXP), Altera (Intel), and Microchip for use with several (real-time) operating systems or its own simple RTOS called NicheTask. It also served as the basis for other TCP/IP stacks, such as SEGGER's emNet (formerly embOS/IP).

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 INFRA:HALT based on the evidence collected during our research, using three main sources:

- A legacy website listing the main customers of InterNiche. According to the website, most of the top industrial automation companies in the world use the stack. Besides those, the website mentions a total of almost 200 device vendors.

- Shodan queries. We queried Shodan, a search engine for connected devices, looking for devices showing some evidence of NicheStack (e.g., application-layer banners). As shown in Figure 16, with a query executed on 08/Mar/2021, we found more than 6,400 instances of devices running NicheStack (using the simple query "InterNiche"). Of those devices, the large majority (6,360) run an HTTP server (query "InterNiche Technologies Webserver"), while the others ran mostly FTP ("Welcome to InterNiche embFtp server"), SSH ("SSH-2.0-InternicheSSHServer (c)InterNiche") or Telnet ("Welcome to InterNiche Telnet Server") servers.

- Forescout Device Cloud. Forescout Device Cloud is the world's largest device knowledge base with 13+ million device fingerprints. We queried it for similar banners as Shodan, as well as other information, based on DHCP signatures, for instance. We found more than 2,500 device instances from 21 vendors. The most affected customer industry vertical is Process Manufacturing, followed by Retail and Discrete Manufacturing.

Q: Where can I find the full INFRA:HALT 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 INFRA:HALT requires patching devices running the vulnerable versions of NicheStack. HCC Embedded has made its official patches available upon request, and device vendors using this software should provide their own updates to customers. Given that patching OT devices is notoriously difficult due to their mission-critical nature, we recommend the following mitigation strategy:

- **Discover and inventory devices running NicheStack.** Forescout Research Labs has released an open-source script that uses active fingerprinting to detect devices running NicheStack. 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 zero-days. Anomalous and malformed traffic should be blocked, or at least alerted of its presence to network operators. **Forescout has released a script for eyeInspect that detects exploitation attempts against the vulnerabilities in INFRA:HALT.**

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 *New Critical Operational Technology Vulnerabilities Found on NicheStack – Mitigation Advised*

FORESCOUT

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