FORESCOUT

NUMBER:JACK **FAQ**

Identify and mitigate risk with Forescout

Q: What is NUMBER:JACK?

A: NUMBER:JACK is a set of 9 new vulnerabilities affecting embedded TCP/IP stacks. The vulnerabilities are related to the same problem, weak Initial Sequence Number (ISN) generation, which can be used to hijack or spoof TCP connections. Ultimately, attackers may be able to leverage those vulnerabilities to:

- Close ongoing connections
- Causing limited denials of service
- Inject malicious data on a device or
- Bypass authentication

ISN's ensure that every TCP connection between two devices is unique and that there are no collisions, so that third parties cannot interfere with an ongoing connection. To guarantee these properties, ISN's must be randomly generated so that an attacker cannot guess an ISN and hijack an ongoing connection or spoof a new one.

Q: How can attackers exploit the NUMBER:JACK vulnerabilities?

A: This type of vulnerability has been used historically to break into general-purpose computers (notoriously by Kevin Mitnick, which led to it be known as the "Mitnick attack").

There are two basic ways to exploit a weak TCP ISN.

1. By predicting the ISN of an existing TCP connection, attackers can close it, thus achieving a Denial-of-Service. Or they can hijack it, thus injecting data into a session. Data can be injected on sensitive unencrypted traffic, such as a telnet session (to inject commands), FTP file downloads (to serve malware) or HTTP responses (to direct the victim to a malicious page).
2. By targeting new TCP connections, attackers may successfully complete a three-way handshake and spoof network packets intended for the victim endpoint or bypass address-based authentication and access control.

Q: What devices are impacted?

A: The impacted stacks are primarily used in embedded devices, potentially widening their impact.

- Four of the vulnerable stacks were discussed in the AMNESIA:33 report. That report showed that these stacks are used by millions of devices. (uIP, FNET, picoTCP, and Nut/Net).
- As for the new vulnerable stacks:
    - According to the 2019 Embedded Markets Study, The Texas Instruments RTOS, which is used in the effected NDKTCPIP is used by 6% of embedded projects.
    - Micrium's uC/OS-II or uC/OS-III are used by 7% of embedded projects.

Q: What does Forescout?

A: Identifying and patching devices running the vulnerable stacks is challenging because it is often unknown which devices run a particular stack, and embedded devices are notoriously difficult to manage and update. That is why we recommend:

- **Discover and inventory devices that run a vulnerable TCP/IP stack.** Forescout Research Labs has released an open-source script that uses active fingerprinting to detect devices running the affected stacks. The script is updated constantly with new signatures. Additionally, Nmap allows the collection of ISN metrics and performs statistical analyses to understand whether a target device suffers from weak ISN generation.

- **Patch when possible.** Monitor progressive patches released by affected device vendors and devise a remediation plan for your vulnerable asset inventory. Forescout can help orchestrate remediation workflows with other IT and security tools for devices that have available patches and can be patched outside of maintenance windows.
- **Segment to mitigate risk.** For vulnerable IoT and OT devices, use segmentation to minimize network exposure and the likelihood of compromise without impacting mission-critical functions or business operations. Segmentation and zoning can also limit the blast radius and business impact if a device is compromised. Forescout eyeSegment can help to restrict external communication paths and isolate or contain vulnerable devices in zones.
- **Deploy IPsec**. End-to-end cryptographic solutions built on top of the Network layer (IPsec) do not require any modifications to a TCP/IP stack in use while allowing to defend against TCP spoofing and connection reset attacks. Unfortunately, this comes at the cost of network bandwidth.

Q: Can Forescout help identify devices with vulnerable stacks?

A: Forescout has the following techniques to identify:

- Nut/Net, FNET, uIP, and picoTCP can all be detected with the AMNESIA:33 SPT
- Nucleus NET, cycloneTCP, NDKTCPIP, and MPLPAB Net vulnerabilities can be detected with the open-source script

Q: Where can I find additional information on NUMBER:JACK?

A: More information can be found in the NUMBER:JACK Blog and the NUMBER:JACK Research Report

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

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

Learn more at Forescout.com