FORESCOUT

NAME:WRECK FAQ

Q: What is NAME:WRECK?

A: Forescout Research Labs, partnering with JSOF Research, disclosed NAME:WRECK, a set of nine Domain Name System (DNS) vulnerabilities that have the potential to cause either Denial of Service (DoS) or Remote Code Execution (RCE), allowing attackers to take target devices offline or control them.

- The widespread use of these stacks and often external exposure of vulnerable DNS clients lead to a dramatically increased attack surface
- The vulnerabilities affect four popular TCP/IP stacks (FreeBSD, IPnet, Nucleus NET and NetX).

Q: What is an example of a potential NAME:WRECK attack scenario?

A: Here is one example of how an attacker might exploit a NAME:WRECK vulnerability:

- An attacker wants to compromise several ultrasound machines for *BrandX*. Knowing the ultrasound connects to download.brandx.com to get firmware updates, the attacker could create a fake firmware that has a backdoor and upload it to a malicious server they own with IP address 1.3.3.7
- The bad actor uses NAME:WRECK to poison the DNS cache of several *BrandX* ultrasounds so that any request to the official site (download.brandx.com) is re-directed to the malicious IP 1.3.3.7
- When the ultrasound requests a firmware update, it connects to the malicious IP 1.3.3.7, downloading and installing the malicious firmware along with the backdoor
- Next, the compromised ultrasound uploads all medical records to a malicious address as instructed by the new malicious firmware

Q: What is the potential impact of NAME:WRECK?

A: NAME:WRECK vulnerabilities impact FreeBSD software used in high-performance servers in millions of IT networks and popular firmware, such as Nucleus NET used in critical IoT/OT devices, as well as NetX and IPnet. An extremely conservative estimate, assuming that 1% of the more than 10 billion deployments discussed below are vulnerable, means that 100 million devices are impacted by NAME:WRECK.

- **Nucleus NET** is deployed in over 3 billion devices such as ultrasound machines, storage systems and critical systems for avionics

- **FreeBSD** is widely used in high-performance servers in millions of IT networks as well as the basis for other well-known open-source projects, such as firewalls and several commercial network appliances
- **NetX** is run by the ThreadX RTOS which is used in wearable fitness products, patient monitors, systems-on-a-chip and several printer models. It is known to have 6.2 billion deployments, with mobile phones, consumer electronics and business automation being the most common product categories.

Q: What sectors are most impacted by NAME:WRECK?

A: Organizations in Healthcare and Government sectors are the most impacted by all three stacks.

Q: What raises the risk level of the NAME:WRECK vulnerabilities?

A: DNS is typically externally accessible, thus creating a large attack surface, and the affected stacks are very popular. For instance, FreeBSD is used in web and storage servers of major organizations, and the other stacks have been used in critical devices for decades.

Q: What should organizations do to mitigate risks?

A: Protection against NAME:WRECK requires patching devices running the vulnerable versions of the IP stacks. FreeBSD, Nucleus NET and NetX have been recently patched, and device vendors using this software should provide their own updates to customers.

Q: How is Forescout Research Labs supporting the cybersecurity community with its research?

A: Disclosing these vulnerabilities to vendors provides much-needed information and education on the impacted products and continues the dialogue in the research community. As part of the NAME:WRECK disclosure, Forescout Research Labs shares with the cybersecurity community the following artifacts:

- An open-source script to detect devices running affected stacks
- A library of DNS anti-patterns to provide researchers and developers worldwide with tools and knowledge needed to tackle similar issues in other stacks
- Upon request (research@forescout.com), samples of malicious traffic captures that researchers and security analysts can use to test their intrusion detection systems
- A standard guide to help developers avoid making the same mistakes while writing future DNS implementations

Q: How does Forescout help mitigate the impact of NAME:WRECK?

A: Forescout helps organizations reduce the risks posed by NAME:WRECK in several ways. Our solutions:

- Discover and inventory devices running the vulnerable stacks
- Enforce segmentation controls and proper network hygiene to mitigate risks
- Monitor progressive patches released by affected device vendors and devise a risk-based remediation plan for your vulnerable assets
- Configure devices to rely on internal DNS servers as much as possible and closely monitor external DNS traffic
- Monitor all network traffic for malicious packets that try to exploit known vulnerabilities or possible zero-day threats affecting DNS, mDNS and DHCP clients.

Q: How can our organization identify vulnerable devices?

A: Forescout eyeSight can identify devices running the operating systems that typically embed the affected stacks: FreeBSD, Nucleus RTOS, ThreadX and VxWorks. Another option is to run the open-source script mentioned above on suspected devices. To know precisely if and how devices with these OSes are affected, their vendors must provide security advisories.