New DNS Vulnerabilities Impacting Healthcare Organizations

Executive Summary

On 12 April 2021, security researchers disclosed a series of medium, high and critical severity DNS vulnerabilities impacting the TCP/IP stacks present in potentially millions of enterprise and consumer devices, with organizations in the healthcare and government sectors impacted most. The flaws could enable threat actors to take affected devices offline or gain control over them. While some patches have been released and mitigations are available, many organizations may encounter hurdles applying the patches where centralized vulnerability management is not an option and many device owners may not even be aware that devices contain these vulnerable TCP/IP stacks.

Report

On 12 April 2021, Forescout and JSOF Research Labs published a joint report revealing nine DNS implementation vulnerabilities dubbed NAME:WRECK affecting four popular TCP/IP stacks. TCP/IP stacks are libraries that vendors add to their firmware to support internet connectivity and other networking functions for their devices. While never visible to end users, these libraries underpin the most basic functions of a device, and any vulnerability there exposes users to remote attacks.

The vulnerabilities allow for either Denial of Service (DoS) or Remote Code Execution (RCE) in products leveraging FreeBSD, IPnet, NetX, and Nucleus NET TCP/IP stacks. Nucleus NET, is commonly used in medical and Internet of Things (IoT) environments. For example, the Nucleus real-time operating system (RTOS) is often implemented in ultrasound machines.

According to Forescout, the widespread deployment and often external exposure of vulnerable DNS clients leads to a dramatically increased attack surface. Furthermore, it is plausible that successful exploitation could enable threat actors to cause significant damage to healthcare facilities by stealing sensitive data, modifying or taking equipment offline for sabotage purposes. Attackers could also tamper with critical building functions in residential or commercial settings such as manipulating HVAC systems, disabling security systems, or tampering with automated lighting systems, and more.

Mitigations

General recommended mitigations for NAME:WRECK include limiting the network exposure of critical vulnerable devices via network segmentation, relying on internal DNS servers and patching devices as soon as vendors release advisories. According to Forescout, complete protection against NAME:WRECK requires patching devices running the vulnerable versions of the IP stacks. FreeBSD, Nucleus NET and NetX have been patched recently (see hyperlinks). Forescout has also made available two open-source tools to help determine if a network device runs a specific embedded TCP/IP stack (Project Memoria Detector) and a tool for detecting issues similar to NAME:WRECK.

See Table 1 for additional NAME:WRECK vulnerability details. Affected versions are listed below:

- FreeBSD (vulnerable version: 12.1)
- IPnet (vulnerable version: VxWorks 6.6)
- NetX (vulnerable version: 6.0.1)
- Nucleus NET (vulnerable version: 4.3)

Analyst Comment

While HC3 has yet to observe successful exploitation of these vulnerabilities in the wild, prioritizing the identification, patching, and mitigation of these vulnerabilities could reduce the risk to an organization especially given their severity and ability to cause significant disruptions to critical operations.

Table 1: NAME:WRECK Vulnerability Details

The table below breaks down all nine vulnerabilities associated with NAME:WRECK with their CVE identification numbers, corresponding TCP/IP stack, affected feature, potential impact and their severity score. The last one has yet to receive a CVE number.

CVE ID	Stack	Affected feature	Potential Impact	Severity Score
CVE-2020-7461	FreeBSD	Message compression	RCE	7.7
CVE-2016-20009	IPnet	Message compression	RCE	9.8
CVE-2020-15795	Nucleus NET	Domain name label parsing	RCE	8.1
CVE-2020-27009	Nucleus NET	Message compression	RCE	8.1
CVE-2020-27736	Nucleus NET	Domain name label parsing	DoS	6.5
CVE-2020-27737	Nucleus NET	Domain name label parsing	DoS	6.5
CVE-2020-27738	Nucleus NET	Message compression	DoS	6.5
CVE-2021-25677	Nucleus NET	Transaction ID	DNS cache poisoning/spoofing	5.3
*	NetX	Message compression	DoS	6.5

References

Aramis, “97% of URGENT/11 and 80% of CDPwn Vulnerable Devices Remain Unpatched Putting Thousands of Organizations at Risk of Attack,” 15 December 2020, https://www.armis.com/urgent11/

Cimpanu, Catalin. “NAME:WRECK vulnerabilities impact millions of smart and industrial devices,” The Record. 13 April 2021. https://therecord.media/namewreck-vulnerabilities-impact-millions-of-smart-and-industrial-devices/

CISA, “ICS Advisory (ICSA-20-343-05) Siemens Embedded TCP/IP Stack Vulnerabilities–AMNESIA:33 (Update C),” ICS-CERT Advisories, 13 April 2021. https://us-cert.cisa.gov/ics/advisories/icsa-20-343-05

Forescout and JSOF, “NAME:WRECK Research Report - Breaking and fixing DNS implementations,” Forescout. 12 April 2021. https://www.forescout.com/company/resources/namewreck-breaking-and-fixing-dns-implementations/

Ilascu, Ionut. “NAME:WRECK DNS vulnerabilities affect over 100 million devices,” BleepingComputer. 13 April 2021. https://www.bleepingcomputer.com/news/security/name-wreck-dns-vulnerabilities-affect-over-100-million-devices/

JSOF, “Ripple20: 19 Zero-Day Vulnerabilities Amplified by the Supply Chain,” JSOF, 16 June 2020, https://www.jsof-tech.com/disclosures/ripple20/