Hive Pro

THREAT ADVISORY

100M Devices being Affected by NAME:WRECK

TA202105

Threat Level Amber

Publish Date – April 14, 2021

Nine Vulnerabilities affecting common TCP/IP stacks which includes FreeBSD, Nucleus NET, Ipnet & NetX can cause Denial of Service (DOS) or Remote Code Execution (RCE). These vulnerabilities are related to Domain Name System clients of affected products. Manipulation of DNS requests and responses allows attacker to control the target devices or take the devices offline. Multiple verticals including healthcare, manufacturing, retail, government are impacted.

Vulnerability Details

CVE ID	Vulnerability Details	Potential Impact	CWE ID
CVE-2021-25677	The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving	DNS cache poisoning	CWE-330
CVE-2020-27009	The DNS domain name record decompression functionality does not properly validate the pointer offset values. The parsing of malformed responses could result in a write past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to execute code in the context of the current process or cause a denial-of-service condition.	RCE	
CVE-2020-15795	The DNS domain name label parsing functionality does not properly validate the names in DNS responses. The parsing of malformed responses could result in a write past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to execute code in the context of the current process or cause a denial-of-service condition.	RCE	
CVE-2020-27736	The DNS domain name label parsing functionality does not properly validate the null-terminated name in DNS-responses. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the read memory.	DOS	CWE-170

Hive Pro

THREAT ADVISORY

100M Devices being Affected by NAME:WRECK

TA202105

CVE ID	Vulnerability Details	Potential Impact	CWE ID
CVE-2020-27737	The DNS response parsing functionality does not properly validate various length and counts of the records. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the memory past the allocated structure.	DOS	CWE-125
CVE-2020-27738	The DNS domain name record decompression functionality does not properly validate the pointer offset values. The parsing of malformed responses could result in a read access past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition.	DOS	CWE-788
CVE-2016-20009	The DNS client has a stack-based overflow on the message decompression function leading to a potential RCE.	RCE	CWE-787
CVE-2020-7461	In FreeBSD 12.1-STABLE before r365010, 11.4-STABLE before r365011, 12.1-RELEASE before p9, 11.4-RELEASE before p3, and 11.3-RELEASE before p13, dhclient(8) fails to handle certain malformed input related to handling of DHCP option 119 resulting a heap overflow. The heap overflow could in principle be exploited to achieve remote code execution. The affected process runs with reduced privileges in a Capsicum sandbox, limiting the immediate impact of an exploit.	RCE	CWE-787
UNASSIGNED	A message-compression bug impacting devices running NetX and can lead to DNS cache- poisoning attacks	DOS	

References

https://cert-portal.siemens.com/productcert/txt/ssa-705111.txt
https://cert-portal.siemens.com/productcert/txt/ssa-669158.txt
https://www.jsof-tech.com/namewreck-dns-vulnerabilities-disclosed-by-jsof-and-forescout/
https://www.forescout.com/company/blog/forescout-and-jsof-disclose-new-dns-vulnerabilities-impacting-millions-of-enterprise-and-consumer-devices/