Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 134 **20-04-2021**

Name: NAME:WRECK DNS Vulnerabilities

Affected Systems: TCP/IP Stacks

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

Threat Classification: Remote code execution

Summary:

About nine vulnerabilities have been reported that affects the implementations of the Domain Name System protocol in TCP/IP network communication stacks run on a wide range of products, from high-performance servers and networking equipment to operational technology systems that monitor and control industrial equipment. Attackers can control heating and ventilation, disable security systems or tamper with automated lighting systems residential and commercial locations**.** An attacker exploiting a single bug may not achieve much but they can potentially wreak havoc by combining them. For instance, they can exploit one flaw to be able to write arbitrary data into sensitive memory locations of a vulnerable device, another to inject code in a packet, and a third one to deliver it to the target.

Severity	**Critical**
Attack Vector	**Network**
Privileges required	**None**

For further details, please visit following link:

- https://us-cert.cisa.gov/ncas/current-activity/2021/04/15/namewreck-dns-vulnerabilities
- https://www.forescout.com/research-labs/namewreck/

Recommendations:

- Please visit following link for the remediation of the aforementioned vulnerabilities:
  - https://www.forescout.com/company/resources/namewreck-breaking-and-fixing-dns-implementations/
  - https://www.forescout.com/research-labs/namewreck/
- Security engineers can use to develop signatures that detect DNS vulnerabilities:
- Discover and inventory devices running the vulnerable stacks
- Enforce segmentation controls and proper network hygiene
- Monitor progressive patches released by affected device vendors
- Configure devices to rely on internal DNS servers
- Monitor all network traffic for malicious packets
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.