The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
05/04/2022

SUBJECT:
A Vulnerability in C Standard Libraries uClibe and uClibe-ng Could Allow for DNS Poisoning

OVERVIEW:
A vulnerability which could allow for DNS poisoning attacks has been discovered in the C standard libraries uClibe and uClibe-ng, which are widely used in IoT products. DNS poisoning enables a subsequent Man-in-the-Middle scenario, which can be used to perform actions like stealing information, forcing authenticated responses, as well as installing malicious firmware.

There is currently no CVE listing, nor further details on affected products, as the research group Nozomi Networks is still working with vendors and library developers in finding a solution.

The MS-ISAC believes that due to various mitigating factors, this vulnerability does not pose an immediate threat to our member base. We would, however, like to share relevant details for your situational awareness.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

To mitigate active enumeration, no details on specific products have been released. However, the libraries in question are known to be used by major router vendors like Linksys and Linux distributions such as Embedded Gentoo. uClibc-ng is a fork designed specifically for the OpenWRT OS used in devices supporting critical infrastructure sectors.

RISK:
Government:

- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability which could allow for DNS poisoning attacks has been discovered in the C standard libraries uClibe and uClibe-ng, which are widely used in IoT products for DNS client interfaces.

These libraries implement DNS requests by calling the internal "__dns_lookup" function, which has the behavior of initializing request transaction IDs at 2, incrementing by one as requests are made, and is then periodically reset back to 2. The predictability of this behavior allows attackers to send unsolicited DNS responses, which can direct the source host to a malicious resolution address if they are able to arrive before the legitimate response. This attack pattern aligns with MITRE ATT&CK technique **T1557: *Man-in-the-Middle***, associated with tactics **TA0009: *Collection*** and **TA0006: *Credential Access***.

Attack complexity is contingent on the following lynchpin factors:

- For DNS poisoning to be successful, the attacker must also supply the correct source port associated with the request. In more modern Linux kernels, this source port is randomized between the range 32768–60999.
    - The vulnerability is more easily exploitable only if the attacker knows that the OS uses a narrow/fixed range, hence the decision to not disclose details of vulnerable products/software.
- In order for the malicious responses to win the race against legitimate ones, the attacker needs considerable bandwidth to send them fast enough while also performing the brute forcing detailed above. Attackers would need infrastructure capable of high concurrency, which may be limited to actors with greater sophistication.
    - Factors providing greater ease of winning the race are high response latency as well as high-volume identical queries, both of which are improbable for an attacker to enumerate.

Because the current lack of information makes it quite difficult for all but the well-resourced and motivated attackers to attempt widespread exploitation, we assess that this vulnerability is currently not likely to present an imminent threat to SLTT agencies. We will update this advisory as new information is released.

Further technical details on the source code analysis and research can be found below in the link to Nozomi Network's article.

RECOMMENDATIONS:
While there are no official patches or recommended mitigations provided by the research group or affected vendors, members can exercise vigilance against the associated TTPs by:

- Blocking DNS traffic from servers outside of a configured allow-list. (**M1037: Filter Network Traffic**)
    - ***Safeguard 4.9: Configure Trusted DNS Servers on Enterprise Assets:*** Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.
    - ***Safeguard 13.4 : Perform Traffic Filtering Between Network Segments:*** Perform traffic filtering between network segments, where appropriate.
- Perform network segmentation such that compromised IoT devices cannot perform lateral movement to workstations or other device groups. If possible, deploy firewalls between devices and the public Internet. (**M1030: Network Segmentation**)
    - ***Safeguard 12.2 : Establish and Maintain a Secure Network Architecture:*** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.
    - ***Safeguard 4.4 : Implement and Manage a Firewall on Servers:*** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

REFERENCES:

Nozomi Networks:
https://www.nozominetworks.com/blog/nozomi-networks-discovers-unpatched-dns-bug-in-popular-c-standard-library-putting-iot-at-risk/

ThreatPost:
https://threatpost.com/dns-bug-millions-routers-iot-risk/179478/