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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
08/06/2021

SUBJECT:
Multiple Vulnerabilities in NicheStack Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in NicheStack, the most severe of which could result in remote code execution. NicheStack are networking protocol libraries specifically designed for embedded systems and are widely used. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of the application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- InterNiche stack versions prior to v4.3
- NicheLite versions prior to v4.3

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:
Multiple vulnerabilities have been discovered in NicheStack, the most severe of which could allow for remote code execution. Details of the vulnerabilities are as follows:

- When parsing DNS domain names, there are no checks on whether a domain name compression pointer is pointing within the bounds of the packet, which may result in an out-of-bounds read. (CVE-2020-25767)
- The routine for parsing DNS response packets does not check the “response data length” field of individual DNS answers, which may cause an out-of-bounds read/write. (CVE-2020-25928)
- The number of queries or responses specified in the DNS packet header is not validated with the query/response data available in the DNS packet, leading to an out-of-bounds read. (CVE-2020-25927)
- The DNS client does not sufficiently randomize transaction IDs, facilitating DNS cache poisoning attacks. (CVE-2020-25926)
- The code that parses ICMP packets relies on an unchecked value of the IP payload size to compute the ICMP checksum, which may result in an out-of-bounds read. (CVE-2020-35683)
- The code that parses TCP packets relies on an unchecked value of the IP payload size to compute the length of the TCP payload within the TCP checksum computation function, which may result in an out-of-bounds read. (CVE-2020-35684)
- TCP ISNs are insufficiently randomized, which may result in TCP spoofing by an attacker. (CVE-2020-35685)
- The TCP urgent data processing function may invoke a panic function, which may result in an infinite loop. (CVE-2021-31400)
- An attacker could send a specially crafted IP packet to trigger an integer overflow due to the lack of IP length validation. (CVE-2021-31401)
- A potential heap buffer overflow exists in the code that parses the HTTP POST request due to lack of size validation. (CVE-2021-31226)
- A potential heap buffer overflow exists in the code that parses the HTTP POST request due to an incorrect signed integer comparison. (CVE-2021-31227)
- An attacker may be able to predict DNS queries’ source port to then send forged DNS response packets, which may be accepted as valid answers. (CVE-2021-31228)
- Unhandled HTTP requests result in an infinite loop that disrupts TCP/IP communication. (CVE-2021-27565)
- The TFTP packet processing function does not ensure that the filename is null-terminated, which may result in a denial-of-service condition. (CVE-2021-36762)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the application. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Run all software as a nonprivileged user with minimal access rights. To reduce the impact of latent vulnerabilities, always run non-administrative software as an unprivileged user with minimal access rights.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- Deploy NIDS to monitor network traffic for signs of anomalous or suspicious activity. This includes but is not limited to requests that include NOP sleds and unexplained incoming

and outgoing traffic. This may indicate exploit attempts or activity that results from successful exploits.
- Do not accept or execute files from untrusted or unknown sources.
- To reduce the likelihood of successful exploits, never handle files that originate from unfamiliar or untrusted sources.
- Implement multiple redundant layers of security. Since this issue may be leveraged to execute code, we recommend memory-protection schemes, such as nonexecutable stack/heap configurations and randomly mapped memory segments. This tactic may complicate exploits of memory-corruption vulnerabilities.

REFERENCES:

Forescout:
https://www.forescout.com/blog/new-critical-operational-technology-vulnerabilities-found-on-nichestack/

CISA:
https://us-cert.cisa.gov/ics/advisories/icsa-21-217-01

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25767
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25926
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25927
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25928
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35683
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35684
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35685
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27565
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31226
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31227
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31228
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31400
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31401
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36762