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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
07/31/2019

SUBJECT:
Multiple Vulnerabilities in Wind River VxWorks Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Wind River's VxWorks Real Time Operating System (RTOS), the most severe of which could allow for remote code execution. VxWorks RTOS is used by various devices across different industry sectors. These devices include but are not limited to SCADA systems, industrial controllers, patient monitoring, MRI machines, firewalls, VoIP phones and printers. Successful exploitation of the most severe of these vulnerabilities could result in a remote attacker obtaining access to a device running a vulnerable OS version.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild, but non-public proof of concept code exists.

SYSTEMS AFFECTED:

- VxWorks 7 (SR540 and SR610)
- VxWorks 6.5-6.9
- Versions of VxWorks using the Interpeak standalone network stack

RISK:
Government:

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

Businesses:

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

Home users: N/A

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Wind River's VxWorks Real Time Operating System, the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:

- One stack overflow vulnerability exists when VxWorks v6.9.4 and above improperly parses IPv4 options (CVE-2019-12256)

- Four memory corruption vulnerabilities exist in VxWorks due to improper handling of TCP's Urgent Point field (CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263)
- One heap overflow vulnerability exists when VxWorks' DHCP client improperly parses DHCP Offer/ACK packets. (CVE-2019-12257)
- One denial of service vulnerability exist when VxWorks v6.5 and above improperly parses malformed TCP options (CVE-2019-12258)
- One denial of service vulnerability exists when VxWorks v6.5 and above improperly parses Reverse ARP reply packets (CVE-2019-12262)
- One denial of service vulnerability exists in VxWorks v6.5 and above's built-in DHCP client accepting any IP address assignment (CVE-2019-12264)
- One denial of service vulnerability exists when VxWorks v6.5 and above receives a specially crafted DHCP response packet to force assignment of a multicast address. This can be followed up by an IGMPv3 membership query packet that results in NULL dereference in network stack (CVE-2019-12259)
- One information disclosure vulnerability exists when VxWorks v6.9.3 and above parses an IGMPv3 membership query report that is fragmented over multiple IP fragments (CVE-2019-12265)

Successful exploitation of the most severe of these vulnerabilities could result in a remote attacker obtaining access to a device running a vulnerable OS version.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches or appropriate mitigations provided by Wind River or product vendor to vulnerable systems immediately after appropriate testing
- Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack.
- Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Wind River:
https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/
https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/security-advisory-ipnet/

Armis:
https://armis.com/urgent11/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12255
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12256
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12257
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12258
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12259
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12260

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12261
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12262
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12263
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12264
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12265

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov

ITS Mississippi Department of Information Technology Services
3771 Eastwood Drive | Jackson, Mississippi 39211-6381

DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited