ABB DOC ID: 3BHS893949
REVISION: A
DATE: 2021-05-06

AC 800PEC – CYBER SECURITY ADVISORY

AC 800PEC platform NAME:WRECK vulnerability

ABBVU-ABBVREP0045- 3BHS893949

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

Affected Products

All ABB products that use the 3rd generation of the AC 800PEC controller – based on the PP E10x processor module – are affected.

Vulnerability ID

ABB ID: ABBVU-ABBVREP0045-3BHS893949

Summary

Forescout Research Labs, partnering with JSOF Research, disclosed NAME:WRECK, a set of Domain Name System (DNS) vulnerabilities that have the potential to cause either Denial of Service (DoS) or Remote Code Execution, allowing attackers to take targeted devices offline or to gain control over them.

The AC 800PEC controllers use VxWorks from WindRiver as the operating system, specifically VxWorks version 6.8. WindRiver does not provide updates to VxWorks version 6.8 anymore. Therefore, the defect is present in all the 3rd generation of the AC 800PEC controller.

The vulnerability could be exploited by an attacker on the same network or on a remote network by spoofing packets.

The Wind River vulnerability CVE number and title is listed in the table below:

CVE	Title	CVSSv3 Score
CVE-2016-20009	Stack overflow may occur in `ipdnsc_decode_name`	9.8

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVE-2016-20009:
CVSS v3 Base Score: 9.8 (Critical)
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3 Link: https://www.first.org/cvss/calculator/3.1

Recommended immediate actions

Either only use IP addresses instead of hostnames for the TRSFTP, SNTP and TRDP services, or setup a trusted DNS server on the same network and make sure a firewall is in place.

Recommended security practices and firewall configurations protect the AC 800PEC controller from attacks that originate from outside the network.

- Use the AC 800PEC within a secure network
- Add a firewall in the network
- Assess the installation specific risk based on this advisory

Vulnerability Details

The vulnerability exists in the TCP/IP stack from VxWorks included in the product versions of the AC 800PEC listed above. An attacker could exploit these vulnerabilities.

The following list contains the description of the vulnerability related to the AC 800PEC controller:

CVE-2016-20009: Stack overflow may occur in `ipdnsc_decode_name`

If an attacker is on the same network as the PEC controller or he can forge spoofed packets when the PEC is connecting to a DNS server on a different network, he could cause Denial of Service (DoS) or Remote Code Execution (RCE). This would allow him to take target devices offline or to take control over them.

All 3rd generation AC 800PEC controller releases are affected.

Frequently Asked Questions

What is the scope of the vulnerability?

The vulnerability relates to Domain Name System (DNS) implementations.

What causes the vulnerability?

The vulnerability is caused by insufficient input data validation in the TCP/IP stack in VxWorks used by the AC 800PEC controller.

What is VxWorks and what is the TCP/IP stack?

VxWorks is the real time operating system used by AC 800PEC controller. It includes e.g. the TCP/IP stack which is the SW component handling the AC 800PEC network communication. IPNet is the name of the TCP/IP stack used in the affected product versions.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take target devices offline or to take control over them.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or by crafting spoofed DNS packets and thus impersonating the remote DNS server. Recommended practices help mitigate such attacks, see section recommended immediate actions above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has access to the DNS server's network could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and the DNS server is part of the trusted network segment. Or to completely forgo using domain names and thus replace the DNS mechanism by only relying on IP addresses.

What does the update do?

There is no update as of now.

When this security advisory was issued, had this vulnerability been publicly disclosed?

The list of vulnerabilities in VxWorks has been publicly disclosed by Wind River: https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2016-20009.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Support

For additional information and support please contact your local ABB service organization. For contact information, see http://new.abb.com/contact-centers.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

For AC 800PEC specific questions please get in contact with the AC 800PEC team (pec@ch.abb.com).