Alcatel·Lucent Enterprise

Alcatel-Lucent Security Advisory No. SA-G0003 Ed. 01
Information about Ripple20 vulnerability

Summary

The JSOF research lab has discovered a series of zero-day vulnerabilities in a widely used low-level TCP/IP software library developed by Treck, Inc. The 19 vulnerabilities, given the name ***Ripple20***, affect hundreds of millions of devices (or more) and include multiple remote code execution vulnerabilities.

Status on Alcatel-Lucent Enterprise products

Alcatel-Lucent Enterprise is not using the TCP/IP stack from Treck Inc. As result, no ALE products are affected by Ripple20 vulnerability.

Description of the vulnerability

Technical Overview

Ripple20 is a set of 19 vulnerabilities found on the Treck TCP/IP stack . Four of the Ripple20 vulnerabilities are rated critical, with CVSS scores over 9 and enable Remote Code Execution. One of the critical vulnerabilities is in the DNS protocol and may potentially be exploitable by a sophisticated attacker over the internet, from outside the network boundaries, even on devices that are not connected to the internet.

A second Whitepaper, to be released following BlackHat USA 2020 will be detailing the exploitation of CVE-2020-11901, a DNS vulnerability, on a Schneider Electric APC UPS device. The other 15 vulnerabilities are in ranging degrees of severity with CVSS score ranging from 3.1 to 8.2, and effects ranging from Denial of Service to potential Remote Code Execution.

Most of the vulnerabilities are true Zero-days, with 4 of them having been closed over the years as part of routine code changes, but remained open in some of the affected devices (3 lower severity, 1 higher). Many of the vulnerabilities have several variants due to the Stack configurability and code changes over the years.

Information about CVE-2020-11896

This vulnerability can be triggered by sending multiple malformed IPv4 packets to a device supporting IPv4 tunneling. It affects any device running Treck with a specific configuration. It can allow a stable remote code execution and has been demonstrated on a Digi International device. Variants of this Issue can be triggered to cause a Denial of Service or a persistent Denial of Service, requiring a hard reset.

Information about CVE-2020-11897

This vulnerability can be triggered by sending multiple malformed IPv6 packets to a device. It affects any device running an older version of Treck with IPv6 support, and was previously fixed as a routine code change. It can potentially allow a stable remote code execution.

Information about CVE-2020-11901

This vulnerability can be triggered by answering a single DNS request made from the device. It affects any device running Treck with DNS support and we have demonstrated that it can be used to perform Remote Code Execution on a Schneider Electric APC UPS. In our opinion this is the most severe of the vulnerabilities despite having a CVSS score of 9.0, due to the fact that DNS requests may leave the network in which the device is located, and a sophisticated attacker may be able to use this vulnerability to take over a device from

outside the network through DNS cache poisoning, or other methods. Thus an attacker can infiltrate the network and take over the device with one vulnerability bypassing any security measures.

The malformed packet is almost completely RFC compliant, and so it will likely be difficult for security products such as firewalls to detect this vulnerability. On very old versions of the Treck stack, still running on some devices, the transaction ID is not randomized making the attack easier.

Information about CVE-2020-11898

Improper Handling of Length Parameter Inconsistency (CWE-130) in IPv4/ICMPv4 component, when handling a packet sent by an unauthorized network attacker.

Possible Exposure of Sensitive Information (CWE-200)

Information about CVE-2020-11900

Possible Double Free (CWE-415) in IPv4 tunneling component when handling a packet sent by a network attacker.

Use After Free (CWE-416)

Information about CVE-2020-11902

Improper Input Validation (CWE-20) in IPv6OverIPv4 tunneling component when handling a packet sent by an unauthorized network attacker.

Possible Out-of-bounds Read (CWE-125)

Information about CVE-2020-11904

Possible Integer Overflow or Wraparound (CWE-190) in Memory Allocation component when handling a packet sent by an unauthorized network attacker.

Possible Out-of-Bounds Write (CWE-787)

Information about CVE-2020-11899

Improper Input Validation (CWE-20) in IPv6 component when handling a packet sent by an unauthorized network attacker.

Possible Out-of-bounds Read (CWE-125), and Possible Denial of Service.

Information about CVE-2020-11903

Possible Out-of-bounds Read (CWE-125) in DHCP component when handling a packet sent by an unauthorized network attacker.

Possible Exposure of Sensitive Information (CWE-200)

Information about CVE-2020-11905

Possible Out-of-bounds Read (CWE-125) in DHCPv6 component when handling a packet sent by an unauthorized network attacker.

Possible Exposure of Sensitive Information (CWE-200)

Information about CVE-2020-11906

Improper Input Validation (CWE-20) in Ethernet Link Layer component from a packet sent by an unauthorized user.

Integer Underflow (CWE-191)

Information about CVE-2020-11907

Improper Handling of Length Parameter Inconsistency (CWE-130) in TCP component, from a packet sent by an unauthorized network attacker

Integer Underflow (CWE-191)

Information about CVE-2020-11909

Improper Input Validation (CWE-20) in IPv4 component when handling a packet sent by an unauthorized network attacker.

Integer Underflow (CWE-191)

Information about CVE-2020-11910

Improper Input Validation (CWE-20) in ICMPv4 component when handling a packet sent by an unauthorized network attacker.

Possible Out-of-bounds Read (CWE-125)

Information about CVE-2020-11911

Improper Access Control (CWE-284) in ICMPv4 component when handling a packet sent by an unauthorized network attacker. Incorrect Permission Assignment for Critical Resource (CWE-732)

Information about CVE-2020-11912

Improper Input Validation (CWE-20) in TCP component when handling a packet sent by an unauthorized network attacker.

Possible Out-of-bounds Read (CWE-125)

Information about CVE-2020-11913

Improper Input Validation (CWE-20) in IPv6 component when handling a packet sent by an unauthorized network attacker.

Possible Out-of-bounds Read (CWE-125)

Information about CVE-2020-11914

"Improper Input Validation (CWE-20) in ARP component when handling a packet sent by an unauthorized network attacker."

Possible Out-of-bounds Read (CWE-125)

Information about CVE-2020-11908

"Improper Input Validation (CWE-20) in ARP component when handling a packet sent by an unauthorized network attacker."

Possible Out-of-bounds Read (CWE-125)

References

JSOF Ripple20 Whitepaper

CVE-2020-11896
Advisory severity
- CVSS Base score: 10.0 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE-2020-11897
Advisory severity
- CVSS Base score: 10.0 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE-2020-11901
Advisory severity
- CVSS Base score: 9.0 - CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE-2020-11898
Advisory severity
- CVSS Base score: 9.1 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

CVE-2020-11900
Advisory severity
- CVSS Base score: 8.2 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

CVE-2020-11902
Advisory severity
- CVSS Base score: 7.3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

CVE-2020-11904
Advisory severity
- CVSS Base score: 7.3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

CVE-2020-11899
Advisory severity
- CVSS Base score: 5.4 - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

CVE-2020-11903
Advisory severity
- CVSS Base score: 6.5 - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVE-2020-11905
Advisory severity
- CVSS Base score: 6.5 - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVE-2020-11906
Advisory severity
- CVSS Base score: 6.3 - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

CVE-2020-11907
Advisory severity
- CVSS Base score: 6.3 - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

CVE-2020-11909
Advisory severity
- CVSS Base score: 5.3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE-2020-11910
Advisory severity
- CVSS Base score: 5.3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE-2020-11911
Advisory severity
- CVSS Base score: 5.3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVE-2020-11912
Advisory severity
- CVSS Base score: 5.3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVE-2020-11913
Advisory severity
- CVSS Base score: 5.3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE-2020-11914
Advisory severity
- CVSS Base score: 4.3 - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE-2020-11908
Advisory severity

- CVSS Base score: 4.3 - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

History

Ed.01 (2020 July 6): creation