Ripple20

CVE IDs & Affected Vendors

June 18, 2020

ATLAS CYBERSECURITY

www.atlas-cybersecurity.com

CVE-2020-11896

- CVSSv3
  - 10
- Description
  - 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.
- Impact
  - Remote code execution

CVE-2020-11897

- CVSSv3
  - 10
- Description
  - 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.
- Potential Impact
  - Out-of-bounds write

CVE-2020-11901

- CVSSv3
  - 9
- Description
  - 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.
- Potential Impact
  - Remote code execution

Additional Vulnerabilities

CVE ID	CVSSv3 Score	Possible Impact
CVE-2020-11898	9.1	Possible Exposure of Sensitive Information (CWE-200)
CVE-2020-11900	8.2	Use After Free (CWE-416)
CVE-2020-11902	7.3	Possible Out-of-Bounds Read (CWE-125)
CVE-2020-11904	5.6	Possible Out-of-Bounds Write (CWE-787)
CVE-2020-11899	5.4	Possible Out-Of-Bounds Read (CWE-125) and Possible Denial of Service
CVE-2020-11903	5.3	Possible Exposure of Sensitive Information (CWE-200)

Additional Vulnerabilities Cont.

CVE ID	CVSSv3 Score	Possible Impact
CVE-2020-11905	5.3	Possible Exposure of Sensitive Information (CWE-200)
CVE-2020-11906	5	Integer Underflow (CWE-191)
CVE-2020-11907	5	Integer Underflow (CWE-191)
CVE-2020-11909	3.7	Integer Underflow (CWE-191)
CVE-2020-11910	3.7	Possible Out-of-Bounds Read (CWE-125)
CVE-2020-11911	3.7	Assignment for Critical Resource (CWE-732)

Additional Vulnerabilities Cont.

CVE ID	CVSSv3 Score	Potential Impact
CVE-2020-11912	3.7	Possible Out-of-Bounds Read (CWE-125)
CVE-2020-11913	3.7	Possible Out-of-Bounds Read (CWE-125)
CVE-2020-11914	3.1	Possible Out-of-Bounds Read (CWE-125)
CVE-2020-11908	3.1	Possible Exposure of Sensitive Information (CWE-200)

Affected Vendors

STATUS: CONFIRMED (15)
B. Braun
Baxter
Caterpillar
Cisco (through Starent)
Digi
Green Hills
HCL Tech
HP
HPE
Intel
Maxlinear (through HLFN)
Rockwell
Sandia National Labs
Schneider Electric/APC
Teradici

STATUS: NOT AFFECTED (9) (as reported by vendor)
Abbott (through Guidant Healthcare)
Amd
GE Healthcare
Laird
Philips
Sandia National Labs
Texas Instruments
Technicolor (Throught CISCO)
Zebra Technologies

STATUS: PENDING (57)		
EMC (now Dell)	Hitachi europe	SAIC
GE general electric (through quadros)	Hlfn	ScriptPro
NASA	Honeywell	Semtech
Verifone	Itron	Sigma Designs
Agilent	Kadak	SimCom Wireless
Airlinq(throug Netsnapper Technologies SARL)	L-3 Chesapeake Sciences Corporation	Starent Networks
Audiocodes	Lockheed martin	Synamedia(Through Cisco)/NDSUK
BAE systems	Marvell	Syncroness
BECK	Maxim Integrated Products	
Broadcom	Memjet	Thinkcom/ThinKom
Capsule (through digi)	MTS Technologies	Tollgrade communications
DASAN Zhone(through vpacket)	Netafim	Ultra Electronics Flightline Systems
Datamax Corporation	Netsnapper Technologies SARL	Vicom
Enghouse (through tollgrade communications)	NVIDIA (through portalplayer)	Videotek
Extreme Networks	Portalplayer	Vocera
Foundry	Qualstar.com	vpacket(now DASAN Zhone)
Fraunhofer IZFP	Quadros	Weibel weibel.dk
Gainspan (telit)	Red lion controls	Western geco
Guidant medical	Redcom	Xilinx
		Zodiac Aerospace