Topic:	**False-positive "Treck TCP/IP stack multiple vulnerabilities (Ripple20)" on E-Series and BEAST**
Product:	BEAST / E18 / E32 / E48 / E60
Distribution:	Partner / Public
Date:	29 September 2020

Reason for Technical Information Bulletin

Vulnerability scanners may report a false-positive detection of "Treck TCP/IP Stack multiple vulnerabilities (Ripple20)" on E-Series/BEAST systems.

The E-Series/BEAST **does not use** the Treck TCP/IP stack. The stack used is proprietary to Nexsan, and is not vulnerable to the publically disclosed "Ripple20" attacks.

The heuristics used to attempt to detect these vulnerabilities are known to have false-positives, which vary between scanners and are being adjusted continuously. Currently known false-positive detections include:

- Tenable Nessus plugin 138615 with "paranoia level 2" enabled (reported as 137702)

Background

In June, the Israeli security research firm JSOF found 19 zero-day vulnerabilities that affect hundreds of millions of Internet of Things (IoT) devices globally. These vulnerabilities were identified in the TCP/IP stack by Ohio-based software company Treck. JSOF called this collection of 19 vulnerabilities Ripple20. For more information on Ripple20, see:

https://www.jsof-tech.com/ripple20/

It is not possible to directly identify the Treck TCP/IP stack, so vulnerability scanners rely on heuristics and fingerprinting to identify potentially-vulnerable devices, which are prone to false-positives.

The "Ripple20" vulnerabilities are due to implementation-specific flaws in the Treck TCP/IP stack. The stack used in the E-Series/BEAST products is unrelated to the Treck TCP/IP stack, and so does not have those specific flaws. Where sufficient technical details of the CVEs have been made publically available, Nexsan have reviewed the E-Series/BEAST TCP/IP stack and confirmed that it is not vulnerable.

Recommendation

Corrective actions for the known false-positive detections are listed below. Detections not listed here are also likely to be false-positives, but should be reported to Nexsan Support (support@nexsan.com) for further investigation.

- **Tenable Nessus 137702 – Treck TCP/IP stack multiple vulnerabilities. (Ripple20)**
  As of 14-Sep-2020, this plugin should only report a vulnerability if "paranoia level 2" is used. Plugin 138615 v1.6 disables this scan by default due to its inaccuracy.
  If "paranoia level 2" is used, create a rule to filter plugin 137702 for all Nexsan E-Series/BEAST IP addresses.

  See https://community.tenable.com/s/feed/0D53a00007FqyYICAZ

This document will be updated as additional detections are identified or resolved.

Technical Support
By Email: support@nexsan.com
By Web: http://www.nexsan.com/support

Part Number: D6200079
Revision: B
Release Date: September 2020

Nexsan 325 E. Hillcrest Drive, Suite 150, Thousand Oaks, CA 91360 | www.nexsan.com