


☐

I'm not robot


reCAPTCHA

Continue

Treck tcp/ip stack library

Skip to main content This advisory should be considered the single source of current, up-to-date, authorized and accurate information from NetApp. Advisory ID: NTAP-20200625-0006 Version: 4.0 Last updated: 07/22/2020 Status: Final. CVEs: CVE-2020-11908, CVE-2020-11903, CVE-2020-11900, CVE-2020-11896, CVE-2020-11898, CVE-2020-11899, CVE-2020-11902, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914 This document is provided solely for informational purposes. All information is based upon NetApp's current knowledge and understanding of the hardware and software products tested by NetApp, and the methodology and assumptions used by NetApp. NetApp is not responsible for any errors or omissions that may be contained herein, and no warranty, representation, or other legal commitment or obligation is being provided by NetApp. © 2017 NetApp, Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of NetApp, Inc. The US Cybersecurity Infrastructure and Security Agency (CISA) has warned of critical vulnerabilities in a low-level TCP/IP software library developed by Treck that, if weaponized, could allow remote attackers to run arbitrary commands and mount denial-of-service (DoS) attacks. The four flaws affect Treck TCP/IP stack version 6.0.1.67 and earlier and were reported to the company by Intel. Two of these are rated critical in severity. Treck's embedded TCP/IP stack is deployed worldwide in manufacturing, information technology, healthcare, and transportation systems. The most severe of them is a heap-based buffer overflow vulnerability (CVE-2020-25066) in the Treck HTTP Server component that could permit an adversary to crash or reset the target device and even execute remote code. It has a CVSS score of 9.8 out of a maximum of 10. The second flaw is an out-of-bounds write in the IPv6 component (CVE-2020-27337, CVSS score 9.1) that could be exploited by an unauthenticated user to cause a DoS condition via network access. Two other vulnerabilities concern an out-of-bounds read in the IPv6 component (CVE-2020-27338, CVSS score 5.9) that could be leveraged by an unauthenticated attacker to cause DoS and an improper input validation in the same module (CVE-2020-27336, CVSS score 3.7) that could result in an out-of-bounds read of up to three bytes via network access. Treck recommends users to update the stack to version 6.0.1.68 to address the flaws. In cases where the latest patches cannot be applied, it's advised that firewall rules are implemented to filter out packets that contain a negative content-length in the HTTP header. The disclosure of new flaws in Treck TCP/IP stack comes six months after Israeli cybersecurity company JSOF uncovered 19 vulnerabilities in the software library — dubbed Ripple20 — that could make it possible for attackers to gain complete control over targeted IoT devices without requiring any user interaction. What's more, earlier this month, Forescout researchers revealed 33 vulnerabilities — collectively called AMNESIA:33 — impacting open-source TCP/IP protocol stacks that could be abused by a bad actor to take over a vulnerable system. Given the complex IoT supply chain involved, the company has released a new detection tool called "project-memoria-detector" to identify whether a target network device runs a vulnerable TCP/IP stack in a lab setting. You can access the tool via GitHub here. **IoT, Software, TCP IP Stack, Vulnerability Read More** 19 vulnerabilities – some of them allowing remote code execution – have been discovered in a TCP/IP stack/library used in hundreds of millions of IoT and OT devices deployed by organizations in a wide variety of industries and sectors. "Affected vendors range from one-person boutique shops to Fortune 500 multinational corporations, including HP, Schneider Electric, Intel, Rockwell Automation, Caterpillar, Baxter, as well as many other major international vendors," say the researchers who discovered the flaws. About the vulnerable TCP/IP software library The vulnerable library was developed by US-based Treck and a Japanese company named Elmic Systems (now Zuken Elmic) in the 1990s. At one point in time, the two companies parted ways and each continued developing a separate branch of the stack/library. The one developed by Treck – Treck TCP/IP – is marketed in the U.S. and the other one, dubbed Kasago TCP/IP, is marketed by Zuken Elmic in Asia. The library's high reliability, performance, and configurability is what made it so popular and widely deployed. "The [Treck TCP/IP] library could be used as-is, configured for a wide range of uses, or incorporated into a larger library. The user could buy the library in source code format and edit it extensively. It can be incorporated into the code and implanted into a wide range of device types," the researchers explained. "The original purchaser could decide to rebrand, or could be acquired by a different corporation, with the original library history lost in company archives. Over time, the original library component could become virtually unrecognizable. This is why, long after the original vulnerability was identified and patched, vulnerabilities may still remain in the field, since tracing the supply chain trail may be practically impossible." The vulnerabilities were discovered by Moshe Kol and Shlomi Oberman from JSOF in the Treck TCP/IP library, and Zuken Elmic confirmed that some of them affect the Kasago library. About the vulnerabilities Collectively dubbed Ripple20, the vulnerabilities (numbered CVE-2020-11896 through CVE-2020-11914) range from critical to low-risk. Four enable remote code execution. Others could be used to achieve sensitive information disclosure, (persistent) denial of service, and more. "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," the researchers noted. "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." The researchers plan to release technical reports on some of them and are scheduled to demonstrate exploitation of the DNS vulnerability on a Schneider Electric APC UPS device at Black Hat USA in August. Coordinated disclosure The Treck TCP/IP library did not receive much attention from security researchers in the past. After JSOF researchers decided to probe it and discovered the flaws, they also discovered that contacting the many, many vendors who implement it was going to be a time-consuming task. Treck was made aware of the vulnerabilities and fixed them, but insisted on contacting clients and users of the code library themselves and to provide the appropriate patches directly. But, since some of the vulnerabilities affect also the Kasago library, JSOF involved multiple national computer emergency response team (CERT) organizations and regulators in the disclosure process. "CERT groups focus on ways to identify and mitigate security risks. For example, they can reach a much larger target group of potential users with blast announcements, 'mass-mailings' that they broadcast to a long list of participating companies to notify them of the potential vulnerability. Once users are identified, mitigation comes into play," the researchers explained. "While the best response might be to install the original Treck patch, there are many situations in which installing the original patch is not possible. CERTs work to develop alternative approaches that can be used to minimize or effectively eliminate the risk, even if patching is not an option." The Ripple20 vulnerabilities have been dubbed thusly because of extent of its impact. "The wide-spread dissemination of the software library (and its internal vulnerabilities) was a natural consequence of the supply chain 'ripple-effect'. A single vulnerable component, though it may be relatively small in and of itself, can ripple outward to impact a wide range of industries, applications, companies, and people," they noted. "The inclusion of the number '20' denotes our disclosure process beginning in 2020, while additionally symbolizing and giving deference to our belief in the potential for additional vulnerabilities to be found from the original 19," they told Help Net Security. The researchers have pointed out that the vulnerability disclosure process, their own efforts to identify users of the Treck library, and the patch/mitigation dissemination process have been immensely aided by Treck, various CERTs, the CISA, and several security vendors (Forescout, CyberMDX). Risk mitigation A number of vendors have confirmed that their offerings are affected by the Ripple20 flaws. JSOF has compiled a list of affected and non affected vendors, which will be constantly updated as additional information becomes available. Device vendors should update the Treck library to a fixed version (6.0.1.67 or higher), while organizations should check their network for affected devices and contact the vendors for more information on how to mitigate the exploitation risk. The researchers will make available, upon request, a script to help companies identify Treck products on their networks. "Fixing these vulnerabilities presents its own set of challenges, even once they've been identified on the network. Some already have patches available. But there are also complicating factors," Forescout CEO and President Michael DeCesare noted. "With these types of supply chain vulnerabilities and embedded components, the vendor that is creating the patch isn't necessarily the one that will release it. That can delay the issuance of a patch. There are also no guarantees that the device vendor is still in business, or that they still support the device. The complex nature of the supply chain may also mean the device is not patchable at all, even if it needs to remain on the network. In such cases, mitigating controls such as segmentation will be needed to limit its risk." Mitigation advice has been provided by CERT/CC and ICS-CERT (CISA). Security updates available for the Treck TCP/IP stack address two critical vulnerabilities leading to remote code execution or denial-of-service. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued an advisory to warn organizations using industrial control systems (ICS) about the risks posed by these flaws. A low-level TCP/IP software library, the Treck TCP/IP stack is specifically designed for embedded systems, featuring small critical sections and a small code footprint. CISA says the product is used worldwide in the critical manufacturing, IT, healthcare and transportation sectors. Last week, a series of four new vulnerabilities that Intel's security researchers discovered in the Treck TCP/IP stack were made public. Two of these were rated critical severity. The most severe of the two is CVE-2020-25066 (CVSS score of 9.8), a heap-based buffer overflow bug in the Treck HTTP Server components that could be abused by attackers to cause denial of service or execute code remotely. Next in line is CVE-2020-27337 (CVSS score of 9.1), an out-of-bounds write in the IPv6 component that could be exploited by an unauthenticated user to cause a DoS condition via network access. Learn more about vulnerabilities in industrial systems at SecurityWeek's ICS Cyber Security Conference and SecurityWeek's Security Summits virtual event series An out-of-bounds read in the DHCPv6 client component of Treck IPv6 could be abused by an unauthenticated user to cause denial-of-service via adjacent network access. The bug is tracked as CVE-2020-27338 (CVSS score of 5.9). The fourth issue, CVE-2020-27336 (CVSS score 3.7), is an improper input validation in the IPv6 component that could lead to an out-of-bounds read of up to three bytes via network access, also without authentication. Users are advised to install the latest version of the affected product (Treck TCP/IP 6.0.1.68 or later), which can be obtained via email from security(at)treck.com. "Treck recommends users who cannot apply the latest patches to implement firewall rules to filter out packets that contain a negative content length in the HTTP header," CISA's advisory reads. To minimize the risk of exploitation, users should ensure that control systems are not accessible from the Internet, they should isolate control system networks and remote devices from the business network and behind a firewall, and should use secure methods, such as VPNs, for remote access. Just as these new vulnerabilities were publicly disclosed, security firm Forescout announced the release of an open-source script that can help identify the use of TCP/IP stacks vulnerable to the recently disclosed AMNESIA:33 set of vulnerabilities. "Although the script has been tested with the four stacks affected by AMNESIA:33 in a lab environment, we cannot guarantee its use to be safe against every possible device. [...] Therefore, we do not recommend using it directly in live environments with mission-critical devices," Forescout notes. Related: 'AMNESIA:33' Vulnerabilities in TCP/IP Stacks Expose Millions of Devices to Attacks Related: Ripple20: Flaws in Treck TCP/IP Stack Expose Millions of IoT Devices to Attacks

16093f7b2f25be---93942902955.pdf
lego ideas book family house instructions
ctrl key stuck in chrome
95615736463.pdf
example of implicit differentiation with solution
scrooge key quotes siave 1
sonatepibanivajisu.pdf
gopofufane.pdf
26300731453.pdf
160a99a0965084---89279015234.pdf
excel vba formula array index match
great gatsby pdf chapter 7
functional movement screen pdf deutsch
78451689093.pdf
advantages and disadvantages of subject centered curriculum pdf
pathophysiology of cardiogenic pulmonary edema pdf
25187233557.pdf
periostitis tibial cronica
the hidden oracle books cool
kolalazogogayuneginola.pdf
domefo.pdf
high school student letter of recommendation template
53898623264.pdf
6165523683.pdf