ExtraHop Threat Research Team Finds One in Three IT Environments Vulnerable to Ripple20 Threat

Report from ExtraHop predicts broad exploitation of devices in a wide range of industries utilising Treck software

SEATTLE – September 10, 2020 – ExtraHop, the leader in cloud-native network detection and response, today issued a report warning of the potential impact of the Ripple20 vulnerabilities if affected software goes undetected and unpatched. Analysing data across its customer base, ExtraHop threat researchers found that 35% of IT environments are vulnerable to Ripple20. The Ripple20 threat is a series of 19 vulnerabilities found in the Treck networking stack, a low-level TCP/IP software library developed by Treck Inc. that is commonly used by device manufacturers across many industries, including utilities, healthcare, government, and academia. The impact of this threat "ripples" through complex software supply chains, making it a difficult vulnerability to mitigate.

The JSOF threat research organisation found the Ripple20 vulnerability (CVE-2020-11901) in June 2020, and unveiled the details to impacted device manufacturers and security vendors to give them ample time to deploy patches and create detections before releasing their findings to the general public. The ExtraHop threat research team studied customer data and discovered vulnerable software in one out of every three IT environments. With industry average dwell times hovering around 56 days, these devices are a ticking time bomb if left alone. ExtraHop experts predict that this exploit will be widely used by attackers as an easy backdoor into networks across industries around the globe.

Click to Tweet: ExtraHop data shows one out of every three IT environments at risk for Ripple20 vulnerability, recommends immediate mitigation action. Read the report for more: https://bit.ly/2FlyP0W

"The devices that utilise the Treck stack are far-reaching with the potential for vast exploitation," said Jeff Costlow, CISO, ExtraHop. "A threat actor could conceivably use this vulnerability to hide malicious code in the embedded devices for an extended period of time, and traditional endpoint or perimeter security solutions like EDR or NGFW will not have visibility into this set of exploits."

Visibility and behavioural analysis of managed and unmanaged devices, including IoT, and visibility into unusual activity from potentially exploited devices within an organisation's east-west traffic, are table stakes for a secure network. Organisations can take a number of steps to help mitigate the risk from Ripple20.

ExtraHop mitigation recommendations include:
Patching: Vendors utilising the Treck Software were given early access to the threat details so they could start producing patches immediately. Unfortunately, a large number of devices have discontinued support which has made it difficult to account for all vulnerable device makes and models.
Removal from Service: If a patch is unavailable for the affected device, it's recommended that organisations consider removing devices from service entirely and replacing them with known secure devices. Removing the device will improve hygiene and compliance, critical for keeping environments secure.
Monitor for Scanning Activity: Before a vulnerable device can be compromised, attackers must first find it. Organisations will need to assess their own practices to understand and monitor which scans are legitimate and which could indicate malicious intent.
Exploit Detection: Because not all vulnerable devices may be identified and patched, it is crucial that organisations detect unusual activity resulting from a Ripple20 exploit as it occurs, such as lateral movement and privilege escalation. Network-based detection is a requirement in this case because embedded devices that use the Treck software will not support endpoint agents.
Isolate Vulnerable Devices: In circumstances where it is not possible to patch affected devices, it is recommended that security teams take the following steps:Verify devices are not publicly accessibleMove devices to a network segment isolated from local subnetsDrop all IP-in-IP traffic destined for affected devicesDrop all IPv6 traffic destined for affected devices
Note on the research:
Data privacy is one of the fundamental questions of our age. ExtraHop passively monitors every interaction on the network then extracts de-identified metadata to be processed by cloud-based machine learning. So, while we can clearly see how prevalent Ripple20 is across the infrastructures we monitor, we do not link that data to any specific customer.

For more information on Ripple20, download the full security advisory: https://www.extrahop.com/resources/whitepapers/ripple20-security-advisory/ or read our blog: https://www.extrahop.com/company/blog/2020/ripple20-vulnerable-devices-and-attacks/

About ExtraHop
ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyses all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customers to identify suspicious behaviour and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI50, Cybercrime Ransomware 25, and SC Media Security Innovator.

Stop Breaches 84% Faster. Get Started at:http://www.extrahop.com/freetrial

Contacts

David Bass
+61 2 9922 6820
mailto: david@basspr.com.au