Sternum and ChargePoint Collaborate to Enhance ChargePoint Home Flex Security

TEL AVIV, ISRAEL, January 23, 2024 /EINPresswire.com/ -- Sternum, the pioneer in embedded IoT security and observability, today announced enhanced security for the ChargePoint Home Flex.

In a comprehensive research project, Sternum identified a potential vulnerability involving the reverse SSH tunnel and deprecated NTP client and HTTP servers. ChargePoint, with its last firmware update, has disabled the HTTP server and updated the NTP client to address the issues. Thanks to the analysis and help of Sternum IoT, ChargePoint was able to correct weaknesses in CPH50, reduce the attack surface and thus improve the security of the product.

“ChargePoint is committed to the security of all customer data, and through this collaboration, we’ve implemented critical enhancements to Home Flex,” said Teza Mukkavilli, Chief Information Security Officer of ChargePoint. “Our focus remains on delivering a convenient, dependable, and safe EV charging experience for all drivers.”

As part of ChargePoint’s commitment to customer security, the company encourages researchers to collaborate with ChargePoint InfoSec to identify potential new vulnerabilities in its products or environment. For more information, please email the InfoSec team at: infosec@chargepoint.com.

Attack methodology
Sternum's experts acquired three different iterations of the ChargePoint Home Flex device. After analyzing a variety of board revisions and through meticulous hardware and software security research, Sternum gained access to the device's firmware and secured a root shell using the JTAG headers on the device.

Findings

The newly discovered vulnerability in the ChargePoint devices revolves around a flaw in the reverse SSH (rSSH) tunnel, established by each unit upon booting. This tunnel, intended to allow ChargePoint to access each charger for telemetry and diagnostics, presents a potential security risk.

The vulnerability arises from the way these devices handle their SSH connections.
Newer devices use a more secure on-demand approach but could still be exploited if the attacker waits for an on-demand connection from the server to the device (which can be initiated by requesting technical support).

Older versions of the software, however, still use an 'always-connect' default setting.
While direct SSH login to the devices is not possible, the vulnerability lies in the potential to forward target ports, such as the HTTP server port, and exploit them for unauthorized access or manipulation.

During the firmware analysis, Sternum identified:
- an outdated HTTP server,
- deprecated NTP client with known vulnerabilities,
- deprecated kernel, and
- device certificates with unlimited expiration time (See figure 1).

Figure 1: See image with this media alert.

Implications of the Vulnerability
Dumping the key pairs from the device implies that an attacker, upon authenticating to ChargePoint's central server, could potentially create their own tunnel. This unauthorized access could extend to each connected charger.

Sternum replicated the client-server setup in its testing facility to validate these findings.

Remediations
Following the discovery, the company actively collaborated with ChargePoint to address the vulnerability, which has been updated in the latest software release.

The update included patching the NTP client, disabling the HTTP Server and changing the SSH connection default to 'on-demand' to mitigate the vulnerability. ChargePoint's fast response to patching these vulnerabilities is a testament to the importance of securing critical infrastructure.

Conclusion
This vulnerability highlights the broader challenges in securing Internet of Things (IoT) devices, especially those linked to critical infrastructure like electric vehicle charging stations. It accentuates the necessity for continual vigilance and regular updates in the IoT landscape to

protect against evolving cybersecurity threats. Sternum's objective is to ensure the ongoing security and reliability of IoT devices and infrastructure, including EV charging systems. The company remains dedicated to collaborating with ChargePoint and other IoT device manufacturers, reinforcing its commitment to safeguard against such vulnerabilities in the future.

Resources:
- Visit http://www.sternumiot.com to learn more
- Book a live demonstration of the Sternum platform at https://sternumiot.com/request-demo/

About Sternum
Founded by ex-8200 (Israel's elite intelligence unit) and Forbes 30UNDER30 Alumni, Sternum offers an embedded platform built for connected devices. By augmenting every device with patented runtime security and granular observability, Sternum provides product, business, security, engineering, and compliance teams with continuous in-field product and fleet monitoring, built-in security, and invaluable business insights. Deployed on millions of devices and serving the world's leading device manufacturers, Sternum enables organizations to improve operational efficiency and achieve business excellence.

Joe Austin
Public Relations
+1 818-332-6166
email us here
Visit us on social media:
Twitter
LinkedIn
