Thales Cinterion EHS8 M2M

CVSS: 6.2

The Thales Cinterion EHS8 M2M (Machine-to-Machine) module is a printed circuit board (PCB) that implements 3G wireless connectivity for IoT devices. The Java ME 3.2 client runtime implements the module's core functionality. IoT manufacturers use this runtime to build applications that communicate via TCP and UDP. Further, the EHS8 module provides TLS/SSL capabilities to secure TCP communication. The module also provides Java over-the-air-provisioning (OTAP) to enable remote device updates.

IBM X-Force Red researchers reported a method for bypassing security measures that protect application-specific data in September 2019 [1]. The researchers working with Thales [2] released a CVE in August 2020. This delay was likely to give Thales time to remediate the issue.

The published CVE, CVE-2020-15858 [3, 4], describes the vulnerability as a directory traversal attack that enables an attacker with physical access to reach the EHS8 module's flash file system directly. Sensitive data such as client application bytecode, credentials such as passwords and tokens, and cryptographic materials such as private keys and public certificates can be accessed unfettered.

While the vulnerability and proof-of-concept attack is not available, Harbor Labs has worked back the appropriate steps and details. IBM X-Force Red identified a vulnerability that affected all EHS8 M2M modules. Therefore, the weakness had to be inherent in the module software design. This finding is not dissimilar to other embedded components that execute software. In particular, a library, tool, or API may be vulnerable.

IBM X-Force Red exploited a directory traversal vulnerability. This type of exposure is due to improper user input sanitization and validation. Harbor Labs consulted the EHS8 M2M Java User's Guide [5] and found a File-Transfer Module. The File-Transfer Module mounts the EHS8 M2M module's flash file system as a Windows drive (e.g., X:) over a physical serial connection. Command-line tools enable the user to interact with the filesystem. The EHS8 M2m user guide also clarifies that some parts of the flash filesystem are secure or "write-only." However, an attacker may bypass software "write-only" checks via a directory traversal attack.

Mitre has provided a CVSS score of 6.2, or medium severity, for this vulnerability. The Attack Vector (AV) and User Interaction (UI) scoring criteria directly impacts the scoring. Specifically, the exploitation of this vulnerability requires physical access and user interaction. If this were a remote attack via the Network, it would have had a High severity of 8.3. Confusingly, the IBM X-Force Red researchers reported that this is a remotely exploitable vulnerability. This fact leads us to believe that the vulnerability and exploit thereof is more complicated than currently disclosed.

In terms of cybersecurity risks, the Cinterion EHS8 M2M module vulnerability may provide an attacker with unauthorized access to remote services and accounts (e.g., an application token or password). It also may allow the attacker to spoof a legitimate device (e.g., a TLS private key). Further, it may enable attacker access to Java bytecode. The attacker may subsequently decompile the decompile and recover intellectual property contained in the code.

Harbor Labs deems this a significant risk for IoT devices that use the Cinterion EHS8 M2M module. Affected devices include include patient health monitors and CGMs (continuous glucose monitors), among other devices that provide remote health monitoring capabilities. In the medical context, the Cinterion EHS8 M2M module vulnerability presents a potential patient safety issue as an attacker may spoof a valid medical device and falsify all data.

Thales has patched the vulnerability and reported it publicly, and a portion of Harbor Labs conclusions have been published in open press [5].

[1] https://securityintelligence.com/posts/new-vulnerability-could-put-iot-devices-at-risk/
[2]https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/resources/security-updates-cinterion-iot-modules
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15858
[3] https://nvd.nist.gov/vuln/detail/CVE-2020-15858
[4]://ftp.matrix.es/mtxm2m/Modems%20M2M/MTX-3G-JAVA%20Family/MTX-3G-JAVA-java_userguide.pdf
[5]https://www.medtechdive.com/news/insulin-pumps-among-millions-of-iot-devices-vulnerable-to-hacker-attacks/584043/