Thales Modules Vulnerability Affecting Devices in the HPH Sector (CVE-2020-15858)

Executive Summary

Researchers recently revealed an information about a vulnerability affecting the electronic chips that enable mobile communication in millions of internet connected devices. The vulnerability affects devices present in various industries including the Healthcare and Public Health (HPH) sector and could allow hackers to hijack the device or access an internal network. A patch was released in February 2020 but many devices in HPH sector are unlikely to have the patch applied.

Report

On August 19, 2020, researchers at IBM X-Force Red identified an Internet of Things (IoT) vulnerability (tracked as CVE-2020-15858) affecting the Thales modules which are used in millions of IoT devices. According to researchers, threat actors could exploit this vulnerability to alter a medical device's reading of a patient's vital signs or manipulate the treatment dosage in medical pumps, for example, and gain access to the central control network to conduct additional attacks. The affected products are manufactured by the French company, Thales, formerly known as Gemalto.

Figure 1. Thales Cinterion EHS8 module used in millions of IoT devices.

Source:

Successful exploitation of the vulnerability bypasses the restrictions in a secure area of the Thales module used for Java code in flash memory allowing full read, write, delete access to the Java code running on the system from both the Original Equipment Manufacturer (OEM) and Thales, resulting in the exposure of all embedded private Java code and sensitive files such as certificates, private keys, or app databases. Using the information stolen from the modules, threat actors could control a device or gain access to the central control network to conduct additional attacks and, in some cases, remotely via 3G.

Thales originally received a report about the vulnerability in September 2019 and released patches for its clients in February 2020. After further testing, Thales confirmed that this vulnerability affects other modules within the same product line of the EHS8 including BGS5, EHS5/6/8, PDS5/6/8, ELS61, ELS81, PLS62 models and further expanding the potential impact of this vulnerability. According to IBM, the patch can be administered two ways – either by plugging in a USB to run an update via software, or by administering an over the air (OTA) update. Affected Thales products include the following modules:

- BGS5 Global 2G Module with Embedded Processing
- EHS5 3G Module
- EHS6 Global 3G Module
- EHS8 Global 3G Module with GPS
- PDS5 Dual Band 3G Module
- PDS6 Global 3G Module
- PDS8 Module
- ELS61 Performance MTC Module
- ELS81 High Speed IoT Module
- PLS62 Performance MTC Module

Analyst Comment

The US-CERT previously released an ICS Medical Advisory (ICSMA-20-170-04) on 23 June 2020 for Baxter Sigma Spectrum Infusion Pumps, indicating medical devices such as infusion pumps are already vulnerable to similar attack. Given the critical nature of the vulnerability, patching vulnerable modules should be considered a priority for organizations in the Healthcare and Public Health (HPH) sector. However, researchers note that applying the patch promptly may be more difficult for devices in the medical sector, where these devices are more heavily regulated and must undergo a lengthy recertification process. While this vulnerability potentially affects millions of IoT devices, it is unknown exactly how many devices are impacted in the HPH sector. Despite this, it is likely that internet-connected medical devices have a Thales module for network communication given its' widespread use.

References

Ionut Ilascu, Researchers detail bug in wireless devices impacting critical sectors (19 August 2020)
https://www.bleepingcomputer.com/news/security/researchers-detail-bug-in-wireless-devices-impacting-critical-sectors/
Adam Laurie and Grzegorz Wypych, New Vulnerability Could Put IoT Devices at Risk (19 August 2020)
https://securityintelligence.com/posts/new-vulnerability-could-put-iot-devices-at-risk/
Thales, IoT Modules, Terminals and Modem Cards
https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-connectivity/products
Thales Press Release, THALES COMPLETES ACQUISITION OF GEMALTO TO BECOME A GLOBAL LEADER IN DIGITAL IDENTITY AND SECURITY (2 April 2019)
https://www.thalesgroup.com/en/group/journalist/press-release/thales-completes-acquisition-gemalto-become-global-leader-digital
Thales Security Updates Web Page
https://cpl.thalesgroup.com/support/security-updates
Mitre, Common Vulnerabilities and Exposures (CVE) Details for CVE-2020-15858 (Created 20200720)
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15858
Drugs, Devices, and the FDA: Part 2: An Overview of Approval Processes: FDA Approval of Medical Devices (2016)
https://www.sciencedirect.com/science/article/pii/S2452302X16300183