SECURITY BULLETIN

Feb. 27, 2018

CareLink 2090 Programmer

Medtronic

Vulnerability Summary

Researchers Billy Rios and Jonathan Butts from WhiteScope LLC have identified vulnerabilities in Medtronic's CareLink™ 2090 Programmer and its accompanying software deployment network.

Medtronic has assessed the vulnerabilities per our internal process. These findings revealed no new potential safety risks based on the existing product security risk assessment. The risks are controlled, and residual risk is acceptable. In an effort to continuously enhance system security, after receiving the vulnerability information from WhiteScope LLC, Medtronic added periodic integrity checks for certain files associated with the software deployment network.

Medtronic customers should continue to follow the security guidance set forth in the Medtronic 2090 CareLink Programmer reference manual. Medtronic has not developed a product update to address these vulnerabilities but has identified compensating controls within this bulletin to help reduce the risk associated with these vulnerabilities.

Medtronic actively reviews its security practices to mitigate risks during premarket development and postmarket use.

Remaining pages of this bulletin include ICS-CERT Advisory ICSMA-18-058-01.

ICSMA-18-058-01 MEDTRONIC 2090 CARELINK PROGRAMMER

February 27, 2018

Overview

Researchers Billy Rios and Jonathan Butts of Whitescope LLC have identified vulnerabilities in Medtronic's 2090 CareLink Programmer and its accompanying software deployment network. The CareLink programmer is a portable computer system used by trained personnel to program and manage cardiac devices in the clinic and procedure room. Medtronic has not developed a product update to address these vulnerabilities but has identified compensating controls within this advisory to help reduce the risk associated with these vulnerabilities.

AFFECTED PRODUCTS

The following 2090 CareLink Programmers are affected:

- 2090 CareLink Programmer, all versions.

IMPACT

Successful exploitation of these vulnerabilities may allow an attacker with physical access to a 2090 Programmer to obtain per-product credentials to the software deployment network. These credentials grant access to the software deployment network, but access is limited to read-only versions of device software applications. No write capability exists with the credentials.

Medtronic has assessed the vulnerabilities and determined that existing controls are sufficient.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment and specific clinical usage.

BACKGROUND

Medtronic is a medical technology, services and solutions company that is headquartered in Dublin, Ireland, and maintains offices around the world.

The affected product, the Medtronic CareLink 2090 Programmer, is used by trained personnel at hospitals and clinics to program and manage Medtronic cardiac devices. According to Medtronic, 2090 CareLink Programmers are deployed across the Healthcare and Public Health sector. These programmers are used worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

Storing Passwords in a Recoverable Format[a] CWE-257

The affected product uses a per-product username and password that is stored in a recoverable format.

CVE-2018-5446 [b] has been assigned to this vulnerability. A CVSS v3 base score of 4.9 has been assigned; the CVSS vector string is (AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).[c]

Relative Path Traversal[d] CWE-23

The affected product's software deployment network contains a directory traversal vulnerability that could allow an attacker to read files on the system.

CVE-2018-5448[e] has been assigned to this vulnerability. A CVSS v3 base score of 4.8 has been assigned; the CVSS vector string is (AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).[f]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could not be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with high skill would be able to exploit these vulnerabilities.

MITIGATION

Medtronic has assessed the vulnerabilities and determined that no new potential safety risks were identified. In order to enhance system security, Medtronic has added periodic integrity checks for files associated with the software deployment network. Additionally, Medtronic has developed server-side security changes that further enhance security. Medtronic reports that they will not be issuing a product update; however, Medtronic has identified compensating controls within this advisory to reduce the risk of exploitation and reiterates the following from the CareLink 2090 Programmer Reference Manual[g]:

- Maintain good physical controls over the programmer. Having a secure physical environment prevents access to the internals of the programmer.
- Only connect the programmer to managed, secure networks.
- Update the software on the programmer when Medtronic updates are available.

NCCIC recommendations, contact information, and document FAQ were redacted for brevity.

a. CWE-257: Storing Passwords in a Recoverable Format, https://cwe.mitre.org/data/definitions/257.html, web site last accessed December 18, 2017.
b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5446, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.
c. CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N, web site last accessed January 6, 2018.
d. CWE-23: Relative Path Traversal, https://cwe.mitre.org/data/definitions/23.html, web site last accessed December 18, 2017.
e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5448, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.
f. CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N, web site last accessed January 6, 2018.
g. Section 1.10.1 of the Medtronic CareLink 2090 Reference Manual (M960587A001) - http://manuals.medtronic.com/content/dam/emanuals/crdm/CONTRIB_224167.pdf