Vulnerability Note VU#948155

Henry Schein Dentrix G5 uses hard-coded database credentials shared across multiple installations

Original Release date: 26 Apr 2013 | Last revised: 13 Jan 2016

Overview

Henry Schein Dentrix G5, a dental practice management software suite, uses hard-coded database access credentials that are shared across multiple installation sites. An attacker who is able to obtain the credentials for one site may be able to gain access to other sites using the same credentials.

Description

Dentrix G5 has uses hard-coded credentials (CWE-798) to access a database back-end. The credentials are the same across installations of Dentrix G5. Sensitive patient information is contained in Dentrix G5 databases. An administrator is unable to change these credentials without breaking access to the back-end database. Henry Schein has provided a vendor statement with additional details about this vulnerability.

Impact

An attacker who is able to obtain the database credentials from one site can potentially access databases on other sites sharing the same credentials. The attacker may need access to the local network or a system with Dentrix G5 installed in order to obtain the credentials, and the attacker would need network access to the database in order to obtain sensitive patient information.

Solution

Apply an Update

Dentrix G5 version 15.1.294 (Dentrix G5.1 Hotfix 1, released 14 Feb 2013) addresses this vulnerability. This update adds a feature to create a unique database back-end password for each Dentrix G5 installation. The update also makes it more difficult to obtain the password from a Dentrix G5 system or the network. Contact Henry Schein customer service for additional information.

Restrict Network Access

As a general good security practice, only allow connections from trusted hosts and networks. Restricting access would prevent an attacker from using the hard-coded credentials from a blocked network location.

Do not allow the Dentrix G5 database to be accessed by unauthorized users on an insecure wireless network. If the Dentrix G5 database is accessible from an insecure wireless network, a remote attacker may be able to gain access using the hard-coded credentials. Wireless access points should be configured to use WPA2 encryption and disable the WiFi Protected Setup (WPS) PIN. Encryption standards such as Wired Equivalent Privacy (WEP) can be easily cracked and should not be relied on to secure wireless networks.

Vendor Information (Learn More)

Vendor	Status	Date Notified	Date Updated

Henry Schein	Affected	15 Oct 2012	28 Apr 2013

If you are a vendor and your product is affected, let us know.

CVSS Metrics (Learn More)

Group	Score	Vector
Base	7.9	AV:A/AC:M/Au:N/C:C/I:C/A:C
Temporal	6.9	E:ND/RL:OF/RC:C
Environmental	2.0	CDP:LM/TD:L/CR:ND/IR:ND/AR:ND

References

- https://www.ftc.gov/news-events/blogs/business-blog/2016/01/ftc-takes-toothless-encryption-claims-dental-practice
- http://wnep.com/2013/12/09/stolen-data-on-thousands-of-williamsport-area-dental-patients/
- http://www.dentrix.com/support/software-updates/g5.aspx
- http://www.dentrix.com/products/dentrix/g5/
- http://cwe.mitre.org/data/definitions/798.html
- http://blog.osvdb.org/tag/henry-schein-practice-solutions/

Credit

Thanks to Justin Shafer for reporting this vulnerability.

This document was written by Jared Allar.

Other Information

CVE IDs:	CVE-2012-4952
Date Public:	22 Nov 2012
Date First Published:	26 Apr 2013
Date Last Updated:	13 Jan 2016
Document Revision:	38

Feedback

If you have feedback, comments, or additional information about this vulnerability, please send us email.