Carestream

Vulnerability Advisory 13032672

Carestream Vulnerability Advisory 13032672

(1) Improper Error Handling in Carestream Vue RIS x11.2

(2) SSL Disabled in Carestream Vue RIS x11.2

Carestream

Vulnerability Advisory 13032672

Product Overview

CARESTREAM Vue RIS improves radiology workflow by automating the patient's diagnostic journey from order entry to results distribution, reducing errors and improving patient care. The Web-based radiology information system is accessible from anywhere, adapts to the needs of multi-site enterprises or hospitals and integrates mammography workflows, peer review and reporting to eliminate disparate systems.

Executive Summary

Carestream is providing notification of the discovery and remediation of two vulnerabilities affecting Carestream Vue RIS v11.2 and earlier running on a Windows 8.1 Machine with IIS/7.5.

An independent Security Researcher discovered and disclosed the vulnerability under a coordinated vulnerability disclosure on July 7th 2018. Carestream has remediated the vulnerability in future versions of the software and provided a work-around for versions affected.

(1) If while contacting the Carestream RIS server there is no Oracle TNS listener available, an HTTP 500 Error will be triggered leaking technical information – database connection strings, information about the back-end application, the local directories. This vulnerability constitutes information leakage and did not directly impact the security posture of the server. However the information may be useful to an attacker in looking for other exploits and vulnerabilities with the application and its underlying infrastructure.

(2) SSL is optional. Messages send from user to the server are unencrypted and could be viewed in plain text with a network monitor.

Recommended Remediation Action

- RIS v11.3 forward | R&D has addressed the information leakage and enabled SSL
- For RIS 11.2 Running Windows 8.1 and IIS 7.2
  - I. Disable "Showdebug messages"
  - II. Enable SSL for client/server communications

Carestream

Vulnerability Advisory 13032672

Support Options

- Please call your local Carestream Support for assistance:
- Visit: https://www.carestream.com/en/us/medical/contact-us/world-wide-contacts
- Open a request through our eService portal.
  https://eservice.carestream.com

Purpose of Advisory

To notify users of a vulnerability and its remediation.

Advisory Status: Advisory published.

Recommendation: Review the **Suggested Actions** section and configure as appropriate.

For more information about this issue, see the following references:

Reference	Identification
Common Vulnerabilities and Exposures	CVE-2018-17891

A CVSS v3 base score of 3.7 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

This advisory discusses the following software:

Affected Software
RIS Client Builds: 11.2x and earlier

Non-Affected Software
RIS Client Builds: 11.3