An official website of the United States government Here's how you know



# ICS Medical Advisory (ICSMA-20-343-01)

More ICS-CERT Advisories

## GE Healthcare Imaging and Ultrasound Products

Original release date: December 08, 2020

## Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

## 1. EXECUTIVE SUMMARY

- **CVSS v3 9.8**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** GE Healthcare
- **Equipment:** GE Imaging and Ultrasound Products
- **Vulnerabilities:** Unprotected Transport of Credentials, Exposure of Sensitive System Information to an Unauthorized Control Sphere

## 2. RISK EVALUATION

Successful exploitation of these vulnerabilities could occur if an attacker gains access to the healthcare delivery organization's (HDO) network. If exploited, these vulnerabilities could allow an attacker to gain access to affected devices in a way that is comparable with GE (remote) service user privileges. A successful exploitation could expose sensitive data such as a limited set of patient health information (PHI) or could allow the attacker to run arbitrary code, which might impact the availability of the system and allow manipulation of PHI.

## 3. TECHNICAL DETAILS

### 3.1 AFFECTED PRODUCTS

The following versions of GE imaging and ultrasound products are affected:

| Modality | Product |
|---|---|

| | |
|---|---|
| MR | 3.0T Signa HDxt / 3.0T Signa HDx, versions HD 16, HD23<br>1.5T Brivo MR355 / Optima MR360, versions SV20.1, SV23.0<br>1.5T Signa HDx / 1.5T Signa HDx, Signa HDi / Signa VIBRANT, versions HD16, HD23 |
| Ultrasound, General Imaging | LOGIQ 5 [BT03], LOGIQ 7 (BT03, BT04, BT06], LOGIQ 9 [BT02, BT03, BT04, BT06] |
| Ultrasound, Cardiovascular | Vivid I [BT06], Vivid 7 {BT02-BT06], EchoPAC (Turnkey) [BT06], Image Vault (Turnkey) [4.3] |
| Ultrasound, Women's Health | Voluson 730 [BT05, BT08] |
| Advanced Visualization | AW 4.0 to AW 4.6, AWS2.0 to AW3.0 |
| **Affected versions of the following can be determined by visiting the GE Customer Portal** | |
| Interventional | Innova 2000, 3100, 4100, 2100-IQ, 3100-IQ, 4100-IQ, 212-IQ, 313-IQ<br>Optima 320, CL320i, CL323i, CL320, 3100<br>Optima IGS 320, 330; Innova IGS 5x0, 6x0, 7x0 |
| Advanced Visualization | AW 4.0 to AW 4.6, AWS2.0 to AW3.0 |
| X-Ray | Brivo XR118, XR383, XR515, XR575; Definium 5000, 6000, 8000, AMX 700; Discovery XR650, XR656, XR656+; Optima XR640, XR646, XR220amx, XR200amx; Precision 500D, WDR1 |
| Mammography | Seno 200D, DS, Essential; Senographe Pristina |
| Computed Tomography | BrightSpeed Elite, Elite Select, Edge, Edge Select<br>Brivo CT385<br>Discovery CT590RT, CT750HD<br>LightSpeed VCT, Pro16, RT16<br>Optima Advance, CT520, CT540, CT660, CT580, CT580RT, CT580W, CT670, CT680 Quantum, Expert & Professional<br>Revolution EVO,HD,ACT, ACTs, CT, Discovery CT, Frontier, Frontier ES |
| Nuclear Medicine, PET/CT | Brivo NM 615<br>Discovery NM 630, NM 750b, NM D530c, NM/CT D570c, NM/CT 670<br>Infinia<br>Discovery NM830, NM/CT 860, NM/CT850, NM/CT 870, MI MI DR, IQ<br>Optima NM/CT 640<br>Ventri<br>Xeleris<br>PET Discovery IQ, IQ upgrade<br>PETrace 800 |

## 3.2 VULNERABILITY OVERVIEW

### 3.2.1 UNPROTECTED TRANSPORT OF CREDENTIALS CWE-523

The affected products may allow specific credentials to be exposed during transport over the network.

CVE-2020-25175 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

### 3.2.2 EXPOSURE OF SENSITIVE SYSTEM INFORMATION TO AN UNAUTHORIZED CONTROL SPHERE CWE-497

The affected products may allow exposed/default credentials to be utilized to access or modify sensitive information.

CVE-2020-25179 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

## 3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Healthcare and Public Health
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** United States

## 3.4 RESEARCHER

Lior Bar Yosef and Elad Luz of CyberMDX reported these vulnerabilities to GE Healthcare.

# 4. MITIGATIONS

GE has identified mitigations for specific products and releases and will take proactive measures to ensure proper configuration of the product firewall protection and change default passwords on impacted devices where possible. GE recommends users refer to the GE Healthcare Product Security Portal for more details on mitigations and how proactive actions may apply to affected devices.

In addition to the product specific recommendations, GE recommends utilizing clinical network security best practices. Suggested clinical best practices include:

- Ensure proper segmentation of the local hospital/clinical network and create explicit access rules based on source/destination IP/port for all connections, including those used for remote support. Specific ports to consider may include those used for TELNET, FTP, REXEC, and SSH
- Utilize IPSec VPN and explicit access rules at the Internet edge before forwarding incoming connections to the local hospital/clinical network.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on us-cert.cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to CISA for tracking and correlation against other incidents.

No known public exploits specifically target these vulnerabilities.

## Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
or incident reporting: https://us-cert.cisa.gov/report

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

---

**This product is provided subject to this Notification and this Privacy & Use policy.**