Medical Devices Hard-Coded Passwords | CISA

Published: 2013-10-29 · Archived: 2026-04-29 02:10:56 UTC

Description

This alert provides information about mitigating a credentials management vulnerability that has been reported across a broad range of medical devices.

SUMMARY

Researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware.

Because of the critical and unique status that medical devices occupy, ICS-CERT has been working in close cooperation with the Food and Drug Administration (FDA) in addressing these issues. ICS-CERT and the FDA have notified the affected vendors of the report and have asked the vendors to confirm the vulnerability and identify specific mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks. ICS-CERT and the FDA will follow up with specific advisories and information as appropriate

The report included vulnerability details for the following vulnerability

Vulnerability Type	Remotely Exploitable	Impact
Hard-coded password	Yes, device dependent	Critical settings/device firmware modification

The affected devices have hard-coded passwords that can be used to permit privileged access to devices such as passwords that would normally be used only by a service technician. In some devices, this access could allow critical settings or the device firmware to be modified.

The affected devices are manufactured by a broad range of vendors and fall into a broad range of categories including but not limited to:

- Surgical and anesthesia devices,
- Ventilators,
- Drug infusion pumps,
- External defibrillators,
- Patient monitors, and
- Laboratory and analysis equipment.

ICS-CERT and the FDA are not aware that this vulnerability has been exploited, nor are they aware of any patient injuries resulting from this potential cybersecurity vulnerability.

MITIGATION

ICS-CERT is currently coordinating with multiple vendors, the FDA, and the security researchers to identify specific mitigations across all devices. In the interim, ICS-CERT recommends that device manufacturers, healthcare facilities, and users of these devices take proactive measures to minimize the risk of exploitation of this and other vulnerabilities. The FDA has published recommendations and best practices to help prevent unauthorized access or modification to medical devices.

- Take steps to limit unauthorized device access to trusted users only, particularly for those devices that are life-sustaining or could be directly connected to hospital networks.
    - Appropriate security controls may include: user authentication, for example, user ID and password, smartcard or biometric; strengthening password protection by avoiding hard-coded passwords and limiting public access to passwords used for technical device access; physical locks; card readers; and guards.
- Protect individual components from exploitation and develop strategies for active security protection appropriate for the device's use environment. Such strategies should include timely deployment of routine, validated security patches and methods to restrict software or firmware updates to authenticated code. Note: The FDA typically does not need to review or approve medical device software changes made solely to strengthen cybersecurity.
- Use design approaches that maintain a device's critical functionality, even when security has been compromised, known as "fail-safe modes."
- Provide methods for retention and recovery after an incident where security has been compromised. Cybersecurity incidents are increasingly likely and manufacturers should consider incident response plans that address the possibility of degraded operation and efficient restoration and recovery.

For health care facilities: The FDA is recommending that you take steps to evaluate your network security and protect your hospital system. In evaluating network security, hospitals and health care facilities should consider:

- Restricting unauthorized access to the network and networked medical devices.
- Making certain appropriate antivirus software and firewalls are up-to-date.
- Monitoring network activity for unauthorized use.
- Protecting individual network components through routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services.
- Contacting the specific device manufacturer if you think you may have a cybersecurity problem related to a medical device. If you are unable to determine the manufacturer or cannot contact the manufacturer, the FDA and DHS ICS-CERT may be able to assist in vulnerability reporting and resolution.
- Developing and evaluating strategies to maintain critical functionality during adverse conditions.

ICS-CERT reminds health care facilities to perform proper impact analysis and risk assessment prior to taking defensive and protective measures.

ICS-CERT also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems

Cybersecurity with Defense-in-Depth Strategies.[a] Although medical devices are not industrial control systems, many of the recommendations from these documents are applicable.

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT and FDA for tracking and correlation against other incidents.

The FDA has also announced a safety communications that highlights the points made in this alert. For additional information see: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm.

```
table.gridtable {
font-family: verdana,arial,sans-serif;
font-size:11px;
color:#333333;
border-width: 1px;
border-color: #666666;
border-collapse: collapse;
}
table.gridtable th {
border-width: 1px;
padding: 8px;
border-style: solid;
border-color: #666666;
background-color: #dedede;
}
table.gridtable td {
border-width: 1px;
padding: 8px;
border-style: solid;
border-color: #666666;
background-color: #ffffff;
}
```
