Safety Communication رسالة سلامة

Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers

<table>
<tr><td>Device/ Product Description:</td><td>Clinical Information Central Stations and Telemetry Servers</td></tr>
<tr><td>Brand:</td><td>• ApexPro Telemetry Server and CARESCAPE Telemetry Server.
• CARESCAPE Central Station (CSCS) version 1.
• CIC Pro Clinical Information Center Central Station version 1.</td></tr>
<tr><td>AFFECTED PRODUCTS:</td><td><table>
<tr><th>DEVICE</th><th>SOFTWARE VERSION</th></tr>
<tr><td>ApexPro Telemetry Server and CARESCAPE Telemetry Server</td><td>4.2 and earlier</td></tr>
<tr><td>CARESCAPE Central Station (CSCS) version 1</td><td>1.x</td></tr>
<tr><td>CIC Pro Clinical Information Center Central Station version 1</td><td>4.x, 5.x</td></tr>
</table></td></tr>
<tr><td>Manufacturer:</td><td>GE Healthcare</td></tr>
<tr><td>Problem:</td><td>Several Cybersecurity vulnerabilities have been identified in certain GE Healthcare Clinical Information Central Stations and Telemetry Servers, that may allow an attacker to remotely take control of the medical device and to silence alarms, generate false alarms and interfere with alarms of patient monitors connected to these devices. Health care providers use GE Clinical Information Central Stations and Telemetry Servers to collect and display data from multiple patient monitoring devices. The data includes physiological status (such as temperature, heartbeat, blood pressure), patient demographic or other nonmedical information.
These vulnerabilities might allow an attack to happen undetected and without user interaction. Because an attack may be interpreted by the affected device as normal network communications, it may remain invisible to existing security measures.</td></tr>
</table>

<table>
<tr><td>Recommendation/ Actions:</td><td>
Recommendations for Health Care Facility Staff (including, Information Technology and Cybersecurity Staff):

• GE Healthcare will be issuing a software patch to address the vulnerabilities and will notify affected customers to deploy them when the patches are ready.

• The risk posed by the vulnerabilities can be reduced by segregating the network connecting the patient monitors with the GE Healthcare Clinical Information Central Stations and Telemetry Servers from the rest of the hospital network, as described in the GE Healthcare documentation for these devices.

• Use firewalls, segregated networks, virtual private networks, network monitors, or other technologies that minimize the risk of remote or local network attacks.

For more information, Please click here.

If you think you had a problem with your device or a device your patient uses, please do not hesitate to report the problem to SFDA through:
NCMDR
Vigilance system
19999 unified call center
</td></tr>
<tr><td>Authorized Representative Details</td><td>
<table>
<tr><td>AR name:</td><td>General Electric Healthcare Arabia</td></tr>
<tr><td>Assigned Contact Person:</td><td>Samer Albawardi</td></tr>
<tr><td>Mobile/Phone:</td><td>0555402028</td></tr>
<tr><td>Email:</td><td>ksa.ra@ge.com</td></tr>
</table>
</td></tr>
</table>