Vulnerabilities Reported by MesaLabs for AmegaView

Executive Summary
MesaLabs’ AmegaView is a continuous monitoring hardware and software platform for laboratories. MesaLabs has announced the discovery of five vulnerabilities, including two critical command injection vulnerabilities, that could allow remote code execution or allow access to devices running AmegaView Versions 3.0 and prior.

Impact to HPH Sector
Although there are currently no public exploits actively targeting these vulnerabilities, the MesaLabs AmegaView continuous monitoring system is used by hospital laboratories, forensics labs, blood banks, IVF labs, pharmacies, and biotech firms. HC3 recommends affected HPH organizations locate vulnerable products behind firewalls, isolate them from the network, and ensure they are only accessible to the Internet using a secure and updated Virtual Private Network (VPN). MesaLabs has announced that it will not release patches to correct the vulnerabilities, although users can upgrade to newer Viewpoint software compatible with AmegaView hardware that is not affected by these vulnerabilities.

- CVE-2021-27447 – CVSS 10/10 – Flaw due to improper neutralization of special elements used in a command, which could allow an attacker to execute arbitrary code.
- CVE-2021-27449 – CVSS 9.9/10 – Flaw due to improper neutralization of special elements used in a command, which could allow an attacker to execute commands in the web server.
- CVE-2021-27445 – CVSS 7.8/10 – Insecure file permissions which could be exploited to elevate privileges on the device.
- CVE-2021-27451 – CVSS 7.3/10 – Improper authentication due to passcodes being generated by an easily reversible algorithm, which could allow an attacker to gain access to the device.
- CVE-2021-27453 – CVSS 7.3/10 – Authentication bypass issue that could allow an attacker to gain access to the web application.

References
Critical Vulnerabilities identified in MesaLabs Laboratory Temperature Monitoring System

ICS Advisory (ICSA-21-147-03)
https://us-cert.cisa.gov/ics/advisories/icsa-21-147-03

Contact Information
If you have any additional questions, please contact us at HC3@hhs.gov.