VULNERABILITY BULLETINS

MesaLabs Laboratory Temperature Monitoring System Critical Vulnerabilities

TLP:WHITE

Jun 08, 2021

ICS Advisory (ICSA-21-147-03) was recently released, which highlighted five critical vulnerabilities that have been identified in the MesaLabs AmegaView that provide continuous monitoring systems that are used in hospital laboratories, forensics labs, and biotech firms. Two of the flaws are susceptible to critical command injection vulnerabilities with CVSS severity scores of 9.9/10 and 10/10, respectively. Other known vulnerabilities include improper authentication, authentication bypass using an alternate path or channel, and improper privilege management. AmegaView products affected by the vulnerabilities include versions 3.0 and prior.

Health-ISAC is distributing this alert to augment efforts supporting the protection of critical infrastructure and the maintenance of organization security posture.

The five critical vulnerabilities were discovered by security researcher Stephen Yackey of Securifera and listed below in order of severity:

- **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.

There are currently no public exploits that specifically target these vulnerabilities. However, MesaLabs has elected to not release patches to correct the vulnerabilities as AmegaView is scheduled for end of life at the conclusion of this year.

Reference(s)	HIPAA Journal, cisa, ISS Source

CVE(s)

CVE-2021-27447 – CVSS 10/10

CVE-2021-27449 – CVSS 9.9/10

CVE-2021-27445 – CVSS 7.8/10

CVE-2021-27451 – CVSS 7.3/10

CVE-2021-27453 - CVSS 7.3/10

Recommendations

All users of the vulnerable products have been advised to upgrade to newer Viewpoint software compatible
with AmegaView hardware. Should this not be possible, or until it is, it is recommended to locate vulnerable products behind firewalls and to isolate them from the network and ensure they are not accessible from the Internet. If remote access is required, Virtual Private Networks (VPNs) should be required for access, and VPNs should be updated to the most current version.

MesaLabs has scheduled AmegaView for end-of-life at the end of 2021. Due to this discontinued service, MesaLabs does not plan to release an update to address these vulnerabilities. MesaLabs recommends users upgrade to the newer ViewPoint software that is compatible with AmegaView hardware.

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.

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.

Sources
HIPAA Journal: Critical Vulnerabilities Identified in MesaLabs Laboratory Temperature Monitoring System

CISA ICS Advisory: (ICSA-21-147-03) - MesaLabs AmegaView

ISS Source MesaLabs: No Fix

Alert ID 0bd05667

View Alert

Tags MesaLabs, AmegaView

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

CISA CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

For Questions or Comments Please email us at toc@h-isac.org