SECURING MD Maryland
INFORMATION SHARING
AND ANALYSIS CENTER

POWERED BY ANOMALI

THREAT BULLETIN

AR20240207-002 [Advisory Report] Threat Actors Continue To Exploit Out Of Date And End Of Life Devices In The Emergency Services Industry

TLP
Clear

DESCRIPTION

TLP:CLEAR = Disclosure is not limited.

Summary

The MD-ISAC continues to receive reports of various network compromises that are a direct result of end of life (EOL) or out of date devices remaining on the network and not being replaced and/or patched. These attacks have impacted various organizations in various industries.

Attached to this bulletin is a report from the Public Safety Threat Alliance regarding a number of critical services that were directly impacted by out of date VMware ESXi servers. While the report discussed the impact to the emergency services industry, this serves as a reminder to all organizations to make sure that all systems exposed to the internet are up to date.

Incident Response

If administrators discover signs of attack or system compromise, the MD-ISAC recommends they:

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report incidents to MD-ISAC via Maryland's 24/7 Operations Center (md-isac@maryland.gov or (410) 697-9700 - option #5).

Reporting and Contact Information

In the case of a cybersecurity incident related to information found in this threat bulletin, Md. Code, Public Safety Article § 14-104.1 (c)(2) and Md. Code, State Finance & Procurement Article § 3.5-406(b)(2)) mandate that you report this via the Maryland Incident Reporting System. It is also recommended that you submit any shareable cyber threat intelligence to the MD-ISAC via the MD-ISAC Threat Intelligence Platform (TIP).

TLP:CLEAR = Disclosure is not limited.

TLP:CLEAR = Disclosure is not limited. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Recipients may share **TLP:CLEAR** information without restriction. Information is subject to standard copyright rules.
For more information about Traffic Light Protocol (TLP) definitions and usage: https://www.cisa.gov/tlp

ATTACHMENTS (1)

Filename	Uploaded By
ESXi Vulnerabilities Actively Exploited Disrupting Emergency Services.pdf	isabella.herman@maryland.gov