Technical Bulletin: VPNFilter

VPNFilter is sophisticated destructive malware capable of both intelligence gathering (e.g., credentials) and destructive behavior (e.g., blocking connectivity). At present, Edgewater Networks does not have any reports of an EdgeMarc Intelligent Edge being affected. However, given the versatility of the malware, this may change.

Edgewater Networks recommends that customers should immediately reset their credentials if they have not already done so and reboot their EdgeMarc Intelligent Edge devices after changing the password.

We will continue to monitor the latest VPNFilter information coming from the security community as well as work quickly to release updates with critical vulnerability patches as they become available.

Refer to our knowledge base for best practices on configuring trusted hosts, passwords, etc.

http://edgewaternetworks.force.com/kb

References

https://blog.talosintelligence.com/2018/05/VPNFilter.html
https://www.us-cert.gov/ncas/current-activity/2018/05/23/VPNFilter-Destructive-Malware
https://www.us-cert.gov/ncas/alerts/TA18-145A