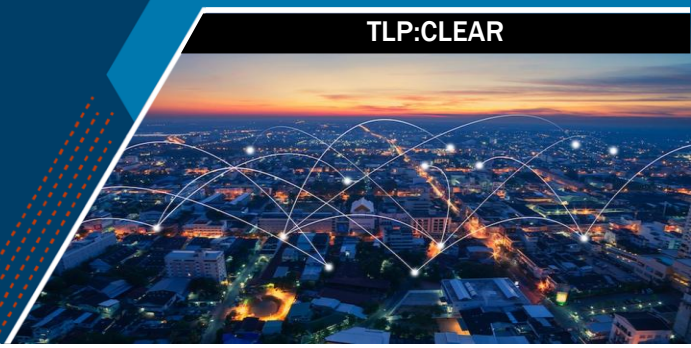
TLP:CLEAR



Reducing the Attack Surface for End-of-Support Edge Devices

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the U.K.'s National Cyber Security Centre (NCSC) are releasing this fact sheet to urge defensive action against malicious cyber activity by nation-state threat actors. Nation-state threat actors exploit end-of-support (EOS) edge devices—including, but not limited to, load balancers, firewalls, routers, and virtual private network (VPN) gateways—to gain network access, maintain presence, and compromise sensitive data.

Organizations using EOS devices are particularly vulnerable to compromise, especially if they are using EOS devices exposed to the public internet or external systems at the network's "edge." CISA's Binding Operational Directive (BOD) 26-02: Mitigating Risk From End-of-Support Edge Devices requires U.S. Federal Civilian Executive Branch (FCEB) agencies to manage the lifecycle of edge devices to defend against malicious cyber activity. Although the BOD 26-02 requirement only applies to FCEB agencies, CISA, FBI, and NCSC strongly encourage organizations to follow the guidance in the BOD and this fact sheet to safeguard systems, data, and operations from nation-state threat actors.

What Are EOS Edge Devices?

Edge devices include technology that resides on the boundary of an organization's network and is accessible from the public internet and other external environments. An edge device becomes an "end-of-support" or "unsupported" device when its manufacturer no longer:

- Monitors it for defects in its software and/or firmware, and
- Updates it with patches for common vulnerabilities and exposures (CVEs), security updates, and software fixes (hotfixes).

EOS edge devices pose significant risks for organizations because threat actors can exploit unresolved security gaps. Nation-state threat actors can exploit these devices as entry points to access modern, supported environments, placing organizations' data, services, and overall security at serious risk. EOS devices may also cause compatibility issues that disrupt productivity.

Mitigations

Organizations should be prepared to respond to malicious cyber activity. As the nation's cyber defense agency, CISA and its partners stand ready to help prepare organizations to respond to and mitigate the impact of malicious cyber activity. CISA and its partners strongly urge all organizations to review BOD 26-02 and implement the following mitigations.

Maintain Asset Inventory and Audits

Keeping track of all devices within a network will equip network defenders with the awareness necessary to protect vulnerable assets.

- Actively scan networks for undocumented and outdated edge devices.
- Maintain an inventory of all edge devices and their respective support timelines.
- Regularly review inventory and EOS dates.
  - Critical infrastructure owners and operators, see Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators.

Replace EOS Edge Devices and Software

Network defenders should proactively monitor for and replace unsupported edge devices to reduce a network perimeter's vulnerability.

- Take prompt action to replace EOS edge devices; as these devices age, managing their risks becomes increasingly challenging and costly.

Install Updates and Patch Known CVEs

Software updates will patch known CVEs; if automatic updates are not enabled, network defenders should proactively monitor for these updates.

- Ensure EOS devices operate on the latest supported software version when immediate replacement is not possible. By using the latest software update, organizations can address CVEs and other known vulnerabilities identified up to the time of the update.
- Enable automatic updates on all devices to install timely patches.

Resources

The following resources provide further guidance on protecting systems from cyber threats linked to EOS software or devices:

- CISA: Edge Device Security webpage provides edge device best practices to help organizations secure their network perimeters against modern cyber threats.
- CISA: Guidance and Strategies to Protect Network Edge Devices offers practical advice and recommendations for protecting edge devices, focusing on minimizing vulnerabilities and improving network resilience.
- CISA: Known Exploited Vulnerabilities Catalog provides a regularly updated list of vulnerabilities actively exploited by threat actors, allowing organizations to prioritize remediation efforts effectively.
- ASD's ACSC: Managing the risks of legacy IT: Executive guidance provides strategies and high-level guidance for executives to mitigate risks stemming from outdated and legacy IT systems.
- ASD's ACSC: Mitigation strategies for edge devices: Practitioner guidance offers detailed technical advice and actionable steps for IT practitioners to enhance the security of edge devices in their networks.

- CISA: No-Cost Cybersecurity Services and Tools lists no-cost services and tools provided by CISA, as well as private and public sector organizations across the cyber community, to strengthen security postures and address cyber risks.
- CISA: Technical Approaches to Uncovering and Remediating Malicious Activity presents detailed technical methodologies and best practices for detecting, analyzing, and addressing malicious activity within networks.
- OASIS: OpenEoX provides robust guidance on the secure lifecycle management and handling of EOS software and associated tools to reduce security vulnerabilities.
- NCSC: Guidance on digital forensics and protective monitoring specifications for producers of network devices and appliances delivers best practices and recommendations for conducting digital forensic investigations and implementing protective monitoring to safeguard network devices against cyber threats.