NIGC Tech Alert

Risk Mitigation Approaches for Unsupported Edge Infrastructure

Persistent cyber threat actors—including those linked to nation-states—are increasingly targeting unsupported edge devices within organizational networks. Because these assets sit at the outer boundary of an IT environment, they are often more exposed, more vulnerable, and more susceptible to compromise. Any device that has reached end of support (EOS) poses an immediate and significant risk to tribal gaming operations. These EOS assets frequently include critical perimeter technologies such as routers, firewalls, and VPN gateways. Their direct exposure to the internet makes them accessible to external attackers, and once manufacturers stop providing security updates, these devices become prime targets for exploitation by advanced threat actors.

Recognizing that this vulnerability affects every sector, the Cybersecurity and Infrastructure Security Agency (CISA) issued Binding Operational Directive (BOD) 26-02, *Mitigating Risks From End of Support Edge Devices* (CISA.gov). Although the directive formally applies to devices supporting federal information systems and networks, all organizations—including tribal gaming operations—should adopt its guidance.

The National Indian Gaming Commission (NIGC) Division of Technology's Technical Regulatory Assessment and Compliance Services (TRACS) teams have identified numerous EOS vulnerabilities during IT vulnerability assessments across tribal gaming operations. These findings highlight the urgent need for tribes to align with the requirements and intent of CISA's BOD 26-02. While NIGC's minimum internal control standards under 25 CFR 543.20 establish baseline IT compliance expectations, each gaming operation is strongly encouraged to develop and maintain robust tribal internal controls and system-level controls tailored to their unique environment. Doing so strengthens cyber hygiene and supports effective mitigation of risks associated with vulnerable assets and infrastructure.

Regardless of the size or structure of the gaming operation, implementing a strong mitigation strategy for EOS devices will significantly reduce vulnerabilities, threats, and overall cyber risk. Most successful cyberattacks exploit conditions that amount to "poor hygiene," such as unpatched known vulnerabilities, weak configuration management, and ineffective device lifecycle management (cisecurity.org).

Every tribal gaming operation should take the following immediate actions to reduce EOS-related risk:

1. **Update all vendor-supported edge devices running EOS software**—including firmware—to a supported version, provided the update does not disrupt mission-critical functions.
2. **Inventory all EOS devices** and maintain continuous visibility into the identification, tracking, and refresh cycles of all edge assets within the organization's IT infrastructure.
3. **Decommission all identified EOS devices as quickly as possible**, replacing them with vendor-supported technologies capable of receiving ongoing security updates.

For more information on BOD 26-02 entitled, Mitigating Risks From End of Support Edge Devices, please find it at https://www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-end-support-edge-devices

For minimum internal control standards, please find the NIGC IT Audit 25 CFR 543.20 Toolkit at https://www.nigc.gov/wp-content/uploads/2026/02/IT-543_20_Toolkit_020626.pdf

April 2026