NIGC Tech Alert

2026 SHAREPOINT COMMON VULNERABILITIES AND EXPOSURES RISK

Traveling around Indian Country we have noticed many operations utilize Microsoft, in this alert we want to discuss CVE's, focusing on SharePoint. Common Vulnerabilities and Exposures (CVE) provide standardized identifiers for publicly known cybersecurity vulnerabilities and exposures, enabling consistent tracking and communication across security tools and databases. The term generally refers to the CVE list, a publicly available catalog of security vulnerabilities maintained by the MITRE Corporation, an independent organization focused on solving complex public interest challenges through systems thinking.

Identifying and mitigating vulnerabilities that attackers can use to compromise applications, systems, and data is one of cybersecurity's central challenges. CVE supports this work by offering a unified framework for cataloging and tracking vulnerabilities, helping organizations strengthen their vulnerability management processes.

Within tribal gaming operations, CVEs may also be incorporated into broader compliance and risk management programs to ensure adherence to Minimum Internal Control Standards and other regulatory requirements set by the National Indian Gaming Commission (NIGC).

During the summer of 2026, organizations have seen an increase in CVEs that pose significant risk if left unpatched. The Cybersecurity and Infrastructure Security Agency (CISA) recently published a list of CVEs currently being actively exploited by malicious actors. Several Microsoft SharePoint Server versions (Subscription Edition, 2019, and 2016) are affected by the following vulnerabilities: CVE-2026-32201, CVE-2026-45659, and CVE-2026-56164. Additionally, Microsoft has disclosed CVE-2026-55040 and CVE-2026-58644, which pose potential risk if unpatched, though they are not currently known to be exploited.

CISA urges all organizations to take immediate action to protect their systems by doing the following:

- Apply the latest patches and security updates from Microsoft
- Verify Antimalware Scan Interface (AMSI) integration in SharePoint
- Hunt for and remediate intrusion artifacts
- Establish tailored logging mechanisms
- Avoid exposing SharePoint Servers to the internet or use a proxy service
- Block external access to SharePoint Central Administration, restrict farm and database communications to required systems

NIGC also recognizes a CVE as a critical control weakness flagged during compliance reviews or internal control assessments. Addressing them is essential to adhering to NIGC and tribal standards, protecting tribal assets, and maintaining regulatory requirements. Regardless of gaming operation, proactively maintaining critical cyber security practices will significantly reduce exploitation from CVEs.

For more information on detection, remediation, and supporting resources, please find it at
CISA Urges Sharepoint Hardening After New Exploitations

To review Microsoft's SharePoint Server security-hardening guidance, please find it at
Plan security hardening for SharePoint Server

If you suspect you have fallen victim to a CVE attack, please inform the Division of Technology (DoT) using the iso@nigc.gov email address. If you have questions concerning any social engineering compromise or any other technical matter, please email ocio@nigc.gov.

July 2026