# NIGC Tech Alert

## Patch Management: Securing The Tribal Gaming IT Enterprise

The threat of attacks on IT systems is always present and one of the many reasons for the need for strong Information Technology system controls and security measures. Despite global recognition that software and firmware patching is effective and hackers regularly seek to exploit unpatched software, many organizations neglect or fail to achieve adequate patch management. Improper update management and arbitrarily applied patches lead to system downtime, application execution failures, and common vulnerability exposures.

Patch management, also called update management, is a component of IT systems management that includes identifying, acquiring, testing and installing patches. The patches include code changes designed to fix bugs, close security holes, or add additional software or hardware features. Installing and applying patches can, in some cases, bring additional risks to an IT infrastructure as patches are programs and may have their own set of unforeseen vulnerabilities. If the patching process is not executed properly, it could lead to system crashes or damaged software and hardware.

Software security updates should be planned and regular applied, especially on critical systems. Keeping software and hardware up to date will reduce the chances of successful malware attacks. This is achieved in part by implementing patch management processes and controls. One control is running regular vulnerability scans of the IT environment to identify vulnerabilities and the systems affected. This type of scan can be used to conduct a vulnerability assessment of the IT environment. If interested, the NIGC IT Audit Team offers technical assistance by performing network vulnerability assessments as a service at all applicable tribal gaming locations.

A recent Open Source Intelligence report from firm Malwarebytes overviews several Cybersecurity and Infrastructure Security Agency (CISA) advisories on current critical vulnerabilities. CISA identified eight critical vulnerabilities that are strongly recommended to be patched by September 8, 2022 due to the likelihood of compromise. The vulnerabilities included Apple iOS, Windows OS and other proprietary systems. Details of those and other vulnerabilities are included in the link below.

Please review the CISA recommendation on eight new critical vulnerabilities at
https://www.malwarebytes.com/blog/news/2022/08/cisa-wants-you-to-patch-these-actively-exploited-vulnerabilities-before-september-8

The National Institute for Standards and Technology (NIST) provides an excellent resource regarding improving patch management. See SP 1800-31, Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways. Additionally, the NIGC offers technical assistance, training courses, IT vulnerability assessments, and other tools and resources to help with patch management and identifying other potentially vulnerable areas to improve security and IT controls and protect tribal resources.

Please view the NIST publication on patch management at
https://www.csrc.nist.gov/publications/details/sp/1800-31/final

Please see NIGC's website for IT Vulnerability Assessment | National Indian Gaming Commission (nigc.gov) information concerning IT Vulnerability Assessment regarding Class II Gaming Systems.