Cyber Intelligence Bulletin from New York State Intelligence Center’s Cyber Analysis Unit

An extremely serious cyber threat has led State and federal cyber security offices to issue a warning to municipal governments. The security vulnerability is found in Netscaler and other Citrix technologies that are commonly used by New York’s municipal governments.

The vulnerability was patched in January. However, attackers have exploited the vulnerability to establish persistent access to networks even after the patch was applied. This “back door” exposes the systems to further malicious activity, and needs to be removed. To address this security vulnerability, the software must not only be patched but a scanner must be run to determine whether the system was compromised prior to the patch being applied.

Local officials are strongly encouraged to contact their Chief Information Officer (CIO), Information Technology (IT) director, or IT support unit to determine whether their municipality uses Citrix technologies. Municipalities that have systems that use Citrix technologies should ensure that the appropriate security patches have been installed and run the “Indicator of Compromise Scanner” (IOC) program to remove the vulnerability.

Information about which systems are vulnerable and a link to the patch and IOC Scanner can be found on the U.S. Department of Homeland Security’s website, [https://www.us-cert.gov/ncas/alerts/aa20-020a](https://www.us-cert.gov/ncas/alerts/aa20-020a). If the scanner returns a positive indication, or if local officials have any questions, they should contact the Cyber Incident Response Team (CIRT) at the NYS Division of Homeland Security and Emergency Services at CIRT@dhses.ny.gov. Additionally, municipalities that suspect that their systems may have been compromised should contact law enforcement.

The NYSIC Cyber Analysis Unit publishes alerts about this and other cyber threats. To be added to their distribution list, please contact them at CAU@nysic.ny.gov.