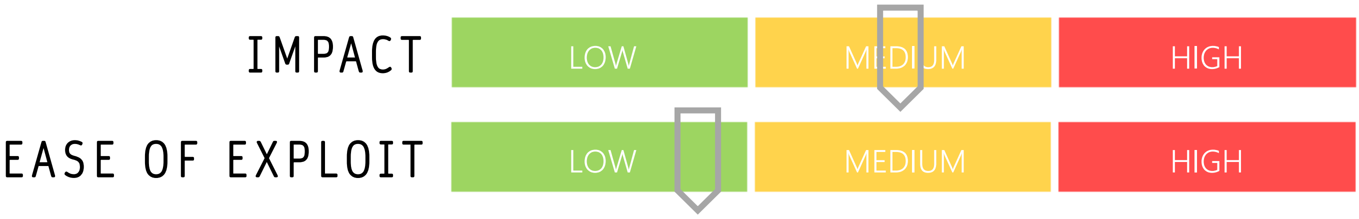
UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00010

CITRIX ADC & GATEWAY BUGS

DATE ISSUED: 10th July 2020



IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	LOW	MEDIUM	HIGH

OVERVIEW

Four bugs present in the Citrix Application Delivery Controller (ADC) and Gateway leave many versions open to code injection, sensitive data leaks and Denial of Service (DoS) attack.

BREAKDOWN

Used for application-aware traffic management and secure remote access, Citrix ADC and Gateway along with the SD-WAN WANOP appliances are potentially vulnerable to unauthenticated access to their management interfaces through Cross Site Scripting (XSS) resulting in unauthorised access to an organizations network. Another attack vector is through targeting Virtual IP addresses, allowing communication with network resources that do not support more than one of the same IP address connections, leaving the Gateway and Authentication servers vulnerable to DoS and unauthorised port scanning on the network. Finally, privilege escalation is possible for a Linux system user with the Citrix Gateway Plug-in. Many of these vulnerabilities have significant barriers in place for those who have followed Citrix recommendations for initial configuration, which will have already positioned themselves to reduce their risk to susceptibility of such attacks.

REMEDIATION STEPS

- Update all Citrix SD-WAN WANOP models 4000-WO, 4100-WO, 5000-WO and 5100-WO with the latest patches
- Update all Citrix ADC and Gateway with the latest security patches
- Review network monitoring and logs for suspicious activity

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/citrix-bugs-allow-unauthenticated-code-injection-data-theft/157214/
	https://threatpost.com/critical-citrix-bug-80000-corporate-lans-at-risk/151444/
Cyberscoop:	https://www.cyberscoop.com/citrix-netscaler-adc-vulnerabilities-july-2020/