U UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00041

FIREFOX HIGH-SEVERITY FLAWS

DATE ISSUED: 28th September 2020

IMPACT	[✓ LOW]	MEDIUM	HIGH
EASE OF EXPLOIT	[✓ HARD]	MEDIUM	EASY

OVERVIEW

Three high-severity flaws in Mozilla's Firefox browser relating to memory usage and the WebGL JavaScript API as well as a number of lower severity flaws have been remediated through the release of Firefox 81 and Firefox ESR78.3.

BREAKDOWN

Mozilla developers have discovered some errors in memory handling could lead to the likes of buffer overflow attacks, which cause an application to behave abnormally and will result in the eventual or sudden application crash. Evidence of possible memory corruption could lead to attacks such as Remote Code Execution). While none of these attacks have been reported as active, as yet and there is little information regarding their exploitability (hence the green rating under Ease of Exploit), pro-actively dealing with them is a far better stance than a reactionary response to an active attack.

REMEDIATION STEPS

- Make sure all devices running Mozilla Firefox web browser are up to date and running the latest version

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/firefox-81-release-bugs/159435/
Mozilla:	https://www.mozilla.org/en-US/firefox/81.0/releasenotes/