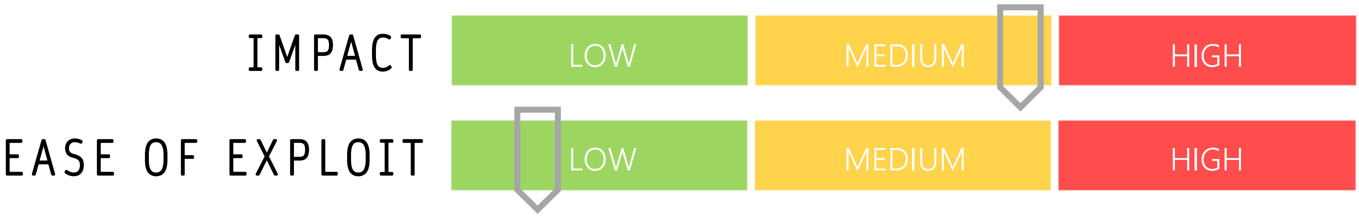
UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00031

CRITICAL CISCO JABBER FLAW FOR WINDOWS

DATE ISSUED: 3rd September 2020



OVERVIEW

Zero interaction required for attackers to carry out Remote Code Execution (RCE) attacks using a critical flaw in the Cisco Jabber videoconferencing software for Windows.

BREAKDOWN

With a large amount of sensitive information being shared over videoconferencing and chat platforms due to the current state with Covid-19, and workforces being shifted to remote working situations, opportunists have increasingly targeted such platforms. Attackers simply send a user a specially crafted Extensible Message and Presence Protocol (XMPP) message that requires no interaction at all and can be launched even when the application is only running in the background. This protocol is XML base and is widely used across both open-source and proprietary devices and software. In some instances, the attacker needs to be on the same XMPP domain as their target. As Jabber does not sanitize incoming HTML messages but rather sends them through a sub-par XSS filter, the filter may be bypassed using the attribute “onanimationstart,” which is called as a JavaScript function at the commencement of an animation playing. Using the attribute and animation, researchers discovered the possibility of attaching malicious HTML tags that could avoid detection by the filter. All an attacker need do is intercept a legitimate XMPP message and modify it with their content to run their executable attached to the animation. CVE-2020-3495

REMEDIATION STEPS

- Apply the latest relevant Cisco security update patches available for your version of Jabber
- Use anti-malware software to detect and respond to any running malware.
- See additional Jabber known vulnerabilities CVE-2020-3430, CVE-2020-3498 & CVE-2020-3537

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/attackers-can-exploit-critical-cisco-jabber-flaw-with-one-message/158942/
Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-UyTKCPGg