Advisory Alert

Alert Number: AAA20210720 **Date:** July 20, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**High**	Use After Free vulnerability
Citrix	**High**	Multiple vulnerabilities

Description

Affected Product	Fortinet
Severity	**High**
Affected Vulnerability	Use After Free vulnerability (CVE-2021-32589)
Description	Fortinet has released security updates addressing Use After Free vulnerability that exists in their product. This flaw allows remote non authenticated attacker to execute unauthorized code as root via sending a specifically crafted request to the fgfm port of the targeted device.
Affected Products	FortiManager versions 5.6.10 and below. FortiManager versions 6.0.10 and below. FortiManager versions 6.2.7 and below. FortiManager versions 6.4.5 and below. FortiManager version 7.0.0. FortiManager versions 5.4.x. FortiAnalyzer versions 5.6.10 and below. FortiAnalyzer versions 6.0.10 and below. FortiAnalyzer versions 6.2.7 and below. FortiAnalyzer versions 6.4.5 and below. FortiAnalyzer version 7.0.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-21-067

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-22919, CVE-2021-22920, CVE-2021-22927)
Description	Citrix has released security updates addressing Multiple vulnerabilities that exists in their products. CVE-2021-22919 - Limited disk space consumption on the appliance. CVE-2021-22920 - SAML authentication hijack through a phishing attack to steal a valid user session. CVE-2021-22927 - Session fixation by an authorized user on SAML SP. Citrix highly recommends to apply necessary workarounds at earliest to avoid issues.
Affected Products	Citrix Application Delivery Controller Citrix Gateway Citrix SD-WAN WANOP
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX319135

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.