# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | Multiple Critical Vulnerabilities in Citrix Gateway and Citrix ADC

**Tracker ID:** TN1116 **Date:** 16/Nov/2022 **Category:** Vulnerability **Industry:** All **Region**: All

### Background

On November 8th, Citrix released a Security Bulletin concerning multiple critical vulnerabilities reported in Citrix Gateway and Citrix ADC that could be exploited by an attacker to bypass the authentication process to gain unauthorized access to Gateway users, take control over victim's RDP sessions via a phishing attack, or perform a brute-force attack on the targeted system.

CVE-2022-27510: Unauthorized access to Gateway user capabilities, is a "Security Bypass" vulnerability affecting Citrix Gateway and Citrix ADC due to an error in the authentication process when the appliance is configured as VPN (Gateway). A remote attacker could bypass the authentication process and gain unauthorized access to Gateway user capabilities. However, to be exploitable the Appliance must be configured as a Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy).

CVE-2022-27516: User login brute force protection functionality bypass, is a "Security Bypass" vulnerability affecting Citrix Gateway and Citrix ADC due to incorrect implementation of the "Max Login Attempts" feature within the VPN (Gateway) or AAA virtual server. Successful exploitation of this vulnerability could allow an attacker to bypass implemented security restrictions and perform a brute-force attack on the targeted system. However, the appliance must be configured as a Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or as a AAA virtual server, and the user lockout functionality “Max Login Attempts” must be configured for either Gateway or AAA virtual server.

CVE-2022-27513: Remote desktop takeover via phishing, is an "Input Validation" vulnerability. This flaw exists in Citrix Gateway and Citrix ADC due to insufficient verification of data authenticity within the RDP proxy. A remote attacker could exploit this vulnerability to take control of a user's RDP sessions via a phishing attack. Successful exploitation of this vulnerability could allow an attacker to configure a VPN(Gateway) and RDP proxy with initial access to the network via SSL-VPN Gateway. The exploitation requires the appliance to be configured as a Gateway (RDP Proxy) and the RDP proxy functionality to be enabled.

These flaws only affect Citrix ADC and Citrix Gateway appliances that are maintained by the customer. Customers using Citrix-managed cloud services do not need to take any action.

### Analysis

| CVE ID | Severity | CVSS Score |
|---|---|---|
| CVE-2022-27510 | Critical | 9.8 |
| CVE-2022-27516 | Critical | 9.8 |
| CVE-2022-27513 | Critical | 9.6 |

# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | Multiple Critical Vulnerabilities in Citrix Gateway and Citrix ADC

**Tracker ID:** TN1116 **Date:** 16/Nov/2022 **Category:** Vulnerability **Industry:** All **Region**: All

### Affected Products and Versions

The following supported versions of Citrix ADC and Citrix Gateway are affected by this vulnerability:

- Citrix ADC and Citrix Gateway 13.1 before 13.1-33.47.
- Citrix ADC and Citrix Gateway 13.0 before 13.0-88.12.
- Citrix ADC and Citrix Gateway 12.1 before 12.1.65.21.
- Citrix ADC 12.1-FIPS before 12.1-55.289.
- Citrix ADC 12.1-NDcPP before 12.1-55.289.

### Recommendations

- Affected customers of Citrix ADC and Citrix Gateway are recommended to install the relevant updated versions of Citrix ADC or Citrix Gateway as soon as possible:
    - Citrix ADC and Citrix Gateway 13.1-33.47 and later releases.
    - Citrix ADC and Citrix Gateway 13.0-88.12 and later releases of 13.0.
    - Citrix ADC and Citrix Gateway 12.1-65.21 and later releases of 12.1.
    - Citrix ADC 12.1-FIPS 12.1-55.289 and later releases of 12.1-FIPS.
    - Citrix ADC 12.1-NDcPP 12.1-55.289 and later releases of 12.1-NDcPP.
- Also, Citrix ADC and Citrix Gateway versions prior to 12.1 are EOL and customers on those versions are recommended to upgrade to one of the supported versions.

### References


- Citrix - Security Bulletin | Critical, CTX463706, Citrix Gateway and Citrix ADC Security Bulletin for CVE-2022-27510 CVE-2022-27513 and CVE-2022-27516, 08th November 2022, Updated: 11th November 2022, External Link (support.citrix.com).


In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471