

Date Posted: 2025/06/30

□Vulnerability Alert□Significant Security Vulnerability in Citrix NetScaler ADC and NetScaler Gateway (CVE-2025-6543)

- Subject: □Vulnerability Alert□Significant Security Vulnerability in Citrix NetScaler ADC and NetScaler Gateway (CVE-2025-6543)
- Content Description:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202506-00000019
 - Citrix NetScaler ADC (formerly Citrix ADC) is a network appliance designed to optimize, secure, and manage enterprise applications and cloud services; NetScaler Gateway (formerly Citrix Gateway) provides secure remote access solutions, allowing users to securely access applications and data from anywhere.
 - Recently, Citrix issued a significant security vulnerability announcement (CVE-2025-6543, CVSS 4.x: 9.2). This is a memory overflow vulnerability that could lead to unexpected control flow changes and denial of service.
 - Note: Affected products NetScaler ADC and NetScaler Gateway 12.1 and 13.0 are End of Life (EoL) products. Citrix recommends upgrading to supported versions.
- Affected Platforms:
 - NetScaler ADC and NetScaler Gateway versions prior to 14.1-47.46 (exclusive)
 - NetScaler ADC and NetScaler Gateway versions prior to 13.1-59.19 (exclusive)
 - NetScaler ADC 13.1-FIPS and NDcPP versions prior to 13.1-37.236-FIPS and NDcPP (exclusive)
- Suggested Measures:
 - NetScaler ADC and NetScaler Gateway 14.1-47.46 (inclusive) and later versions, NetScaler ADC and NetScaler Gateway 13.1-59.19 (inclusive) and later versions, NetScaler ADC 13.1-FIPS and NDcPP 13.1-37.236-FIPS and NDcPP (inclusive) and later versions
- References:
 - <https://www.twcert.org.tw/tw/cp-169-10221-b5f6f-1.html>

Computer and Communications Center
Network Systems Division Respectfully

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250630_04

Last update: **2025/06/30 11:21**