

Date Posted: 2026/04/02

[Vulnerability Alert] Critical Security Vulnerability Found in Citrix NetScaler ADC and NetScaler Gateway (CVE-2026-3055)

- Subject Explanation: [Vulnerability Alert] Critical Security Vulnerability Found in Citrix NetScaler ADC and NetScaler Gateway (CVE-2026-3055)
- Content Description:
 - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202603-00000021
 - Citrix NetScaler ADC (formerly Citrix ADC) is a network device designed to optimize, secure, and manage enterprise applications and cloud services; NetScaler Gateway (formerly Citrix Gateway) provides a secure remote access solution, allowing users to safely access applications and data from any location.
 - Recently, Citrix released a critical security advisory (CVE-2026-3055, CVSS 4.x: 9.3). This is an Out-of-bounds Read vulnerability caused by insufficient input validation, leading to over-reading of memory.
- Impacted Platforms:
 - NetScaler ADC and NetScaler Gateway versions prior to 14.1-60.58 (exclusive)
 - NetScaler ADC and NetScaler Gateway versions prior to 13.1-62.23 (exclusive)
 - NetScaler ADC FIPS and NDcPP versions prior to 13.1-37.262 (exclusive)
- Suggested Measures:
 - Please update to the following versions:
 - NetScaler ADC and NetScaler Gateway versions 14.1-60.58 and later, NetScaler ADC and NetScaler Gateway versions 13.1-62.23 and later, NetScaler ADC FIPS and NDcPP versions 13.1-37.262 and later
- References:
 1. <https://www.twcert.org.tw/tw/cp-169-10799-be596-1.html>

Computer and Communication Center
Network Systems Division

From:

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

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260402_22



Last update: **2026/04/02 09:37**