

# **NCSC** Advisory

Critical Vulnerabilities in Citrix NetScaler ADC & Gateway CVE-2025-5777, CVE-2025-5349

19th, June 2025

**STATUS: TLP:CLEAR** 

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.





# Description

CVE ID: CVE-2025-5777, CVE-2025-5349

Published: 2025-06-17

Vendor: Citrix

**Products:** Netscaler ADC, Netscaler Gateway

CVSS Score<sup>1</sup>: 9.3, 8.7

### **Products Affected**

Product	Version
NetScaler ADC and NetScaler Gateway	< 14.1-43.56
NetScaler ADC and NetScaler Gateway	< 13.1-58.32
NetScaler ADC 13.1-FIPS and 13.1- NDcPP	< 13.1-37.235
NetScaler ADC 12.1-FIPS	< 12.1-55.328

# **Impact**

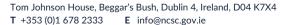
Insufficient input validation leading to memory overread on the NetScaler Management Interface NetScaler ADC and NetScaler Gateway. Successful exploitation of this vulnerability in various versions of NetScaler ADC and NetScaler Gateway can allow unauthenticated attackers to conduct memory overread over the network.

Common Weakness Enumeration (CWE)<sup>2</sup>: CWE-125: CWE-125 Out-of-bounds Read, CWE-284: Improper Access Control

Known Exploited Vulnerability (KEV) catalog<sup>3</sup>: No

Used by Ransomware Operators: N/A





<sup>&</sup>lt;sup>1</sup> https://www.first.org/cvss/

<sup>&</sup>lt;sup>2</sup> https://cwe.mitre.org

<sup>&</sup>lt;sup>3</sup> https://www.cisa.gov/known-exploited-vulnerabilities-catalog

#### TLP: CLEAR

An Roinn Comhshaoil, Aeráide agus Cumarsáide Department of the Environment, Climate and Communications



### Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from NetScaler.

- https://nvd.nist.gov/vuln/detail/CVE-2025-5777
- https://nvd.nist.gov/vuln/detail/CVE-2025-5349
- https://www.cve.org/CVERecord?id=CVE-2025-5777
- https://www.cve.org/CVERecord?id=CVE-2025-5349
- https://support.citrix.com/supporthome/kbsearch/article?articleNumber=CTX693420



