An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2607200215

NCSC Advisory

Vulnerabilites in Citrix Secure Access Client for Windows and Citrix Endpoint Analysis Client for Windows

CVE-2026-53565 and CVE-2026-53566

20 July 2026

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 IDs: CVE-2026-53565 and CVE-2026-53566

Published: 2026-07-14

Vendor: Citrix

Products: Citrix Secure Access Client for Windows, Citrix Endpoint Analysis Client for Windows

CVSS Scores[1]**:** 8.5 and 6.8

Products Affected

Product	Version
Citrix Secure Access Client for Windows	0 < 26.6.1.20
Citrix Endpoint Analysis Client for Windows	0 < 26.5.1.7

Impact

CVE-2026-53565

An improper privilege management vulnerability has been identified in the Citrix Secure Access Client for Windows and the Citrix Endpoint Analysis Client for Windows. A successful exploit could allow an attacker to gain elevated privileges on an affected system.

This issue affects the Citrix Secure Access Client for Windows before 26.6.1.20 and the Citrix Endpoint Analysis Client for Windows before 26.5.1.7.

Common Weakness Enumeration (CWE)[2]: CWE-269: Improper Privilege Management

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE-2026-53566

An out-of-bounds read vulnerability has been identified in the Citrix Secure Access Client for Windows. A successful exploit could allow an attacker to read memory outside the intended buffer, potentially exposing sensitive information or causing the application to behave unexpectedly.

This issue affects the Citrix Secure Access Client for Windows before 26.6.1.20.

Common Weakness Enumeration (CWE): CWE-125: Out-of-bounds read

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

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 Citrix.

- https://nvd.nist.gov/vuln/detail/CVE-2026-53565
- https://nvd.nist.gov/vuln/detail/CVE-2026-53566
- https://www.cve.org/CVERecord?id=CVE-2026-53565
- https://www.cve.org/CVERecord?id=CVE-2026-53566
- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696734