



CVE-2025-15610

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-15610 |
| State | PUBLISHED |
| Assigner | OpenText |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-15 17:17:00 UTC |
| Updated | 2026-04-15 17:17:00 UTC |
| Description | Deserialization of untrusted data vulnerability in OpenText, Inc RightFax on Windows, 64 bit, 32 bit allows Object Injection.7 |

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from security@opentext.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-502 | CWE-502 CWE-502 Deserialization of untrusted data

| Version | Source | Type | Score | Severity | Vector |
|---------|-----------------------|-----------|-------|----------|---|
| 4.0 | security@opentext.com | Secondary | 9.3 | CRITICAL | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |
| 4.0 | CNA | CVSS | 9.3 | CRITICAL | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|------------------------------|--------------------------|--------------------------------------|-------------------------|
| CNA | OpenText Inc | RightFax | affected 16.6 16.6 Update7136 custom | Windows, 64 bit, 32 bit |
| CNA | OpenText Inc | RightFax | affected 20.2 20.2 Update5705 custom | Windows, 64 bit, 32 bit |
| CNA | OpenText Inc | RightFax | affected 21.2 21.2.1.2678 custom | Windows, 64 bit, 32 bit |
| CNA | OpenText Inc | RightFax | affected 22.2 22.2.2.347 custom | Windows, 64 bit, 32 bit |
| CNA | OpenText Inc | RightFax | affected 23.4 23.4.2.853 custom | Windows, 64 bit, 32 bit |
| CNA | OpenText Inc | RightFax | affected 24.4 24.4.2.853 custom | Windows, 64 bit, 32 bit |
| CNA | OpenText Inc | RightFax | affected 25.4 25.4.2.347 custom | Windows, 64 bit, 32 bit |

References

| Reference | Source | Link | Tags |
|--|--|--------------------------------------|---------------------|
| support.opentext.com/csm | security@opentext.com | support.opentext.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

