# Local Privilege Escalation via OpenSSL configuration file in Insight Agent

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-6482 |
| **State** | PUBLISHED |
| **Assigner** | rapid7 |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-04-17 06:16:30 UTC |
| **Updated** | 2026-04-17 15:38:09 UTC |
| **Description** | The Rapid7 Insight Agent (versions > 4.1.0.2) is vulnerable to a local privilege escalation attack that allows users to gain SY |

## Risk And Classification

**Primary CVSS:** v4.0 8.5 HIGH from cve@rapid7.com

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

**EPSS:** 0.000140000 probability, percentile 0.026650000 (date 2026-04-20)

**Problem Types:** CWE-829 | CWE-829 CWE-829 Inclusion of functionality from untrusted control sphere

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | cve@rapid7.com | Secondary | 8.5 | HIGH | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L/E:P/C... |
| 4.0 | CNA | CVSS | 8.5 | HIGH | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L/E:P |

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

Low

Sub Conf.

High

Sub Integrity

High

Sub Availability

Low

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/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 | Rapid7 | Insight Agent | affected 4.1.0.2 custom | Windows |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| docs.rapid7.com/insight/release-notes-2026-april | cve@rapid7.com | docs.rapid7.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Dell Security Assurance Team (en)

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

**CVE.report and Source URL Uptime Status** status.cve.report