Metasploit Pro on Windows: Local Privilege Escalation via OpenSSL Configuration File Loading

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

Summary

CVE	CVE-2026-7373
State	PUBLISHED
Assigner	rapid7
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 03:16:23 UTC
Updated	2026-05-15 03:16:23 UTC
Description	Rapid7 Metasploit Pro is vulnerable to a local privilege escalation attack that allows users to gain SYSTEM level control of a

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:H/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

Problem Types: CWE-284 | CWE-427 | CWE-829 | CWE-829 CWE-829 Inclusion of Functionality from Untrusted Control Sphere | CWE-427 CWE-427 Uncontrolled Search Path Element | CWE-284 CWE-284 Improper Access Control

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:H/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:H/E:P

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

Low

Sub Conf.

High

Sub Integrity

High

Sub Availability

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:H/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	Metasploit Pro	affected 5.0.0 custom	Windows

References

Reference	Source	Link	Tags
docs.rapid7.com/insight/metasploit-pro-release-notes	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: Andrea Intilangelo (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-23T14:05:00.000Z	Vulnerability reported to Rapid7
CNA	2026-04-24T03:54:00.000Z	Rapid7 acknowledged receipt and confirmed remediation in progress
CNA	2026-04-28T23:55:00.000Z	CVE-2026-7373 reserved
CNA	2026-05-14T05:49:00.000Z	CVE record updated

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

Free CVE JSON API cve.report/api

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