# CVE-2026-5463

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-5463 |
| **State** | PUBLISHED |
| **Assigner** | TuranSec |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-04-03 05:16:24 UTC |
| **Updated** | 2026-04-03 05:16:24 UTC |
| **Description** | Command injection vulnerability in console.run_module_with_output() in pymetasploit3 through version 1.0.6 allows attacke |

## Risk And Classification

**Primary CVSS:** v4.0 9.3 CRITICAL from 309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L/E:X/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-77 | CWE-77 CWE-77 Improper neutralization of special elements leading to command injection

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | 309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c | Secondary | 9.3 | CRITICAL | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA |
| 4.0 | CNA | CVSS | 9.3 | CRITICAL | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA |
| 3.1 | 309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c | Secondary | 8.6 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L |
| 3.1 | CNA | CVSS | 8.6 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L |
| 2.0 | 309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c | Secondary | 7.5 | | AV:N/AC:L/Au:N/C:P/I:P/A:P |
| 2.0 | CNA | CVSS | 7.5 | | AV:N/AC:L/Au:N/C:P/I:P/A:P |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

High

Availability

Low

Sub Conf.

Low

Sub Integrity

High

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L/E:X/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

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

High

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Dan McInerney | Pymetasploit3 | affected 1.0.6 python | Not specified |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| pypi.org/project/pymetasploit3 | 309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c | pypi.org | |
| github.com/DanMcInerney/pymetasploit3 | 309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c | github.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:** Abdivasiyev Sunnatillo (en)

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