CVE-2019-5624

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-5624
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-30 17:29:00 UTC
Updated	2023-02-01 02:22:00 UTC
Description	Rapid7 Metasploit Framework suffers from an instance of CWE-22, Improper Limitation of a Pathname to a Restricted Direc

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rapid7	Metasploit	All	All	All	All

References

Reference	Source	Link
Zip import directory traversal mitigation by sgonzalez-r7 · Pull Request #11716 · rapid7/metasploit-framework · GitHub	CONFIRM	github.c
On insecure zip handling, Rubyzip and Metasploit RCE (CVE-2019-5624) · Doyensec's Blog	MISC	blog.doy
Metasploit Release Notes Archive - April 2019	CONFIRM	help.rap
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered by Doyensec, and reported privately by Luca Carettoni.

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