CVE-2020-7385

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-7385
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-23 16:15:00 UTC
Updated	2021-05-14 14:00:00 UTC
Description	By launching the drb_remote_codeexec exploit, a Metasploit Framework user will inadvertently expose Metasploit to the sa

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
Fixes and updates for the DRuby RCE module by zeroSteiner · Pull Request #14300 · rapid7/metasploit-framework · GitHub	MISC
Metasploit Release Notes Archive - October 2020	MISC
Remove the DRuby remote code execution module by zeroSteiner · Pull Request #14335 · rapid7/metasploit-framework · GitHub	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered by Jeff Dileo of NCC Group, and reported to Rapid7 via Rapid7's coordinated vulnerability disclosure process, detailed here: https://www.rapid7.com/.well-known/security.txt

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