CVE-2020-5741

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

Summary

CVE	CVE-2020-5741
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-08 13:15:00 UTC
Updated	2021-12-14 21:50:00 UTC
Description	Deserialization of Untrusted Data in Plex Media Server on Windows allows a remote, authenticated attacker to execute arbi

Risk And Classification

EPSS: 0.360190000 probability, percentile 0.971440000 (date 2026-05-17)

CISA KEV: Listed on 2023-03-10; due 2023-03-31; ransomware use Unknown

Problem Types: CWE-502

CISA Known Exploited Vulnerability

Vendor	Plex
Product	Media Server
Name	Plex Media Server Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://forums.plex.tv/t/security-regarding-cve-2020-5741/586819; https://nvd.nist.gov/vuln/detail/CVE-2020-5741

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Plex	Media Server	All	All	All	All
Application	Plex	Plex Media Server	All	All	All	All
Application	Plex	Plex Media Server	All	All	All	All

References

Reference	Source	Link	Tags

Reference	Source	Link	Tags
Plex Unpickle Dict Windows Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
Plex Media Server Authenticated Python Deserialization / RCE (Windows)	MISC	www.tenable.com	Exploit, Third Party Advi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

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**