FreePBX api module Command Injection via GraphQL

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

Summary

CVE	CVE-2026-40520
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 13:16:20 UTC
Updated	2026-04-21 16:20:24 UTC
Description	FreePBX api module version 17.0.8 and prior contain a command injection vulnerability in the initiateGqlAPIProcess() funct

Risk And Classification

Primary CVSS: v4.0 8.6 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/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-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA
4.0	CNA	CVSS	8.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	FreePBX	Api	affected 17.0.8 semver	Not specified
CNA	FreePBX	Api	unaffected 5f194e39a47e5481e8947f9694304d32724175f6 git	Not specified

References

Reference	Source	Link	Ta

github.com/FreePBX/api/blob/5f194e39a47e5481e8947f9694304d32724175f6/Api...	disclosure@vulncheck.com	github.com	
github.com/FreePBX/api/commit/5f194e39a47e5481e8947f9694304d32724175f6	disclosure@vulncheck.com	github.com	
github.com/FreePBX/api/blob/5f194e39a47e5481e8947f9694304d32724175f6/Api...	disclosure@vulncheck.com	github.com	
www.vulncheck.com/advisories/freepbx-api-module-command-injection-via-graphql	disclosure@vulncheck.com	www.vulncheck.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

Vendor Comments And Credit

Discovery Credit

CNA: M. Cory Billington of theyhack.me (en)

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