CVE-2025-53681

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

Summary

CVE	CVE-2025-53681
State	PUBLISHED
Assigner	fortinet
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 18:16:35 UTC
Updated	2026-05-12 18:57:02 UTC
Description	An improper neutralization of special elements used in an SQL Command ("SQL Injection&") vulnerability [CWE-89] vulnera

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from psirt@fortinet.com

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

Problem Types: CWE-89 | CWE-89 Execute unauthorized code or commands

Version	Source	Type	Score	Severity	Vector
3.1	psirt@fortinet.com	Secondary	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	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

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	Fortinet	FortiMail	affected 7.6.0 7.6.3 semver	Not specified
CNA	Fortinet	FortiMail	affected 7.4.0 7.4.5 semver	Not specified
CNA	Fortinet	FortiMail	affected 7.2.0 7.2.8 semver	Not specified

References

Reference	Source	Link	Tags
fortiguard.fortinet.com/psirt/FG-IR-26-132	psirt@fortinet.com	fortiguard.fortinet.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Upgrade to FortiMail version 7.6.4 or above Upgrade to FortiMail version 7.4.6 or above Upgrade to FortiMail version 7.2.9 or above Fortinet remediated this issue in FortiMail Cloud version 25.2 and hence customers do not need to perform any action.

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