Vaelsys VaelsysV4 Web interface vgrid_server.php execute_DataObjectProc os command injection

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

Summary

CVE	CVE-2025-8259
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-28 06:15:23 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability was identified in Vaelsys VaelsysV4 up to 5.1.0/5.4.0. Affected by this issue is the function execute_DataObj

Risk And Classification

Primary CVSS: v4.0 5.5 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/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-77 | CWE-78 | CWE-78 OS Command Injection | CWE-77 Command Injection

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	5.5	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C.
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vuldb.com	Secondary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vaelsys	Vaelsys	4.1.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Vaelsys	VaelsysV4	affected 5.0	Not specified
CNA	Vaelsys	VaelsysV4	affected 5.1	Not specified
CNA	Vaelsys	VaelsysV4	affected 5.1.0	Not specified
CNA	Vaelsys	VaelsysV4	affected 5.2	Not specified
CNA	Vaelsys	VaelsysV4	affected 5.3	Not specified
CNA	Vaelsys	VaelsysV4	affected 5.4.0	Not specified
CNA	Vaelsys	VaelsysV4	unaffected 5.1.1	Not specified
CNA	Vaelsys	VaelsysV4	unaffected 5.4.1	Not specified

References

Reference	Source	Link	Tags
vuldb.com/vuln/317847	cna@vuldb.com	vuldb.com	
vaelsys.github.io/security-advisory/advisories/VSEC_V4_2025_07_0001.html	cna@vuldb.com	vaelsys.github.io	
github.com/waiwai24/0101/blob/main/CVEs/Vaelsys/Remote_Code_Execution_in...	cna@vuldb.com	github.com	Exploit, Third Part
vuldb.com/vuln/317847/cti	cna@vuldb.com	vuldb.com	
vuldb.com/submit/616920	cna@vuldb.com	vuldb.com	

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

Vendor Comments And Credit

Discovery Credit

CNA: waiwai24 (VulDB User) (en)

CNA: security_vaelsys (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-07-26T02:00:00.000Z	VulDB entry created
CNA	2026-03-20T00:00:00.000Z	Advisory disclosed
CNA	2026-04-15T09:13:10.000Z	VulDB entry last update

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