Vaelsys VaelsysV4 Web interface vgrid_server.php weak hash

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

Summary

CVE	CVE-2025-8260
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-28 06:15:25 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A security flaw has been discovered in Vaelsys VaelsysV4 up to 5.1.0/5.4.0. This affects an unknown part of the file /grid/vg

Risk And Classification

Primary CVSS: v4.0 1.3 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/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-327 | CWE-328 | CWE-328 Use of Weak Hash | CWE-327 Risky Cryptographic Algorithm

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	1.3	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	cna@vuldb.com	Secondary	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
3.0	CNA	DECLARED	3.1	LOW	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	2.1		AV:N/AC:H/Au:S/C:P/I:N/A:N
2.0	CNA	DECLARED	2.1		AV:N/AC:H/Au:S/C:P/I:N/A:N/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

None

Availability

None

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/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
github.com/waiwai24/0101/blob/main/CVEs/Vaelsys/Unauthorized_Access_Lead...	cna@vuldb.com	github.com	Exploit, Third Party
vuldb.com/vuln/317848	cna@vuldb.com	vuldb.com	
vuldb.com/vuln/317848/cti	cna@vuldb.com	vuldb.com	
vuldb.com/submit/616922	cna@vuldb.com	vuldb.com	
vaelsys.github.io/security-advisory/advisories/VSEC_V4_2025_07_0002.html	cna@vuldb.com	vaelsys.github.io	

vaelsys.github.io/security-advisory/advisories/VDB-[illegible]	cna@vuldb.com	vaelsys.github.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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	2026-04-15T09:07:00.000Z	VulDB entry last update

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