Linksys RE6250/RE6300/RE6350/RE6500/RE7000/RE9000 upload.cgi cgiMain os command injection

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

Summary

CVE	CVE-2025-9575
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-08-28 18:15:34 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.0(

Risk And Classification

Primary CVSS: v4.0 2.1 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/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	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vuldb.com	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	6.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

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:L/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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Linksys	Re6250	-	All	All	All
Operating System	Linksys	Re6250 Firmware	1.0.04.001	All	All	All
Hardware	Linksys	Re6300	-	All	All	All
Operating System	Linksys	Re6300 Firmware	1.2.07.001	All	All	All
Hardware	Linksys	Re6350	-	All	All	All
Operating System	Linksys	Re6350 Firmware	1.0.04.001	All	All	All
Hardware	Linksys	Re6500	-	All	All	All
Operating System	Linksys	Re6500 Firmware	1.0.013.001	All	All	All
Hardware	Linksys	Re7000	-	All	All	All
Operating System	Linksys	Re7000 Firmware	1.1.05.003	All	All	All
Hardware	Linksys	Re9000	-	All	All	All
Operating System	Linksys	Re9000 Firmware	1.0.04.002	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Linksys	RE6250	affected 1.0.013.001	Not specified
CNA	Linksys	RE6250	affected 1.0.04.001	Not specified
CNA	Linksys	RE6250	affected 1.0.04.002	Not specified

CNA	Linksys	RE6250	affected 1.1.05.003	Not specified
CNA	Linksys	RE6250	affected 1.2.07.001	Not specified
CNA	Linksys	RE6300	affected 1.0.013.001	Not specified
CNA	Linksys	RE6300	affected 1.0.04.001	Not specified
CNA	Linksys	RE6300	affected 1.0.04.002	Not specified
CNA	Linksys	RE6300	affected 1.1.05.003	Not specified
CNA	Linksys	RE6300	affected 1.2.07.001	Not specified
CNA	Linksys	RE6350	affected 1.0.013.001	Not specified
CNA	Linksys	RE6350	affected 1.0.04.001	Not specified
CNA	Linksys	RE6350	affected 1.0.04.002	Not specified
CNA	Linksys	RE6350	affected 1.1.05.003	Not specified
CNA	Linksys	RE6350	affected 1.2.07.001	Not specified
CNA	Linksys	RE6500	affected 1.0.013.001	Not specified
CNA	Linksys	RE6500	affected 1.0.04.001	Not specified
CNA	Linksys	RE6500	affected 1.0.04.002	Not specified
CNA	Linksys	RE6500	affected 1.1.05.003	Not specified
CNA	Linksys	RE6500	affected 1.2.07.001	Not specified
CNA	Linksys	RE7000	affected 1.0.013.001	Not specified
CNA	Linksys	RE7000	affected 1.0.04.001	Not specified
CNA	Linksys	RE7000	affected 1.0.04.002	Not specified
CNA	Linksys	RE7000	affected 1.1.05.003	Not specified
CNA	Linksys	RE7000	affected 1.2.07.001	Not specified
CNA	Linksys	RE9000	affected 1.0.013.001	Not specified
CNA	Linksys	RE9000	affected 1.0.04.001	Not specified
CNA	Linksys	RE9000	affected 1.0.04.002	Not specified
CNA	Linksys	RE9000	affected 1.1.05.003	Not specified
CNA	Linksys	RE9000	affected 1.2.07.001	Not specified

References

Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	vuldb.com	Third Party A
github.com/wudipjq/my_vuln/blob/main/Linksys/vuln_13/13.md	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Exploit, Third
vuldb.com	cna@vuldb.com	vuldb.com	Permissions
vuldb.com	cna@vuldb.com	vuldb.com	Third Party A
github.com/wudipjq/my_vuln/blob/main/Linksys/vuln_13/13.md	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Exploit, Third
www.linksys.com	cna@vuldb.com	www.linksys.com	Product

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

Vendor Comments And Credit

Discovery Credit

CNA: Bond_yes (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-08-28T00:00:00.000Z	Advisory disclosed
CNA	2025-08-28T02:00:00.000Z	VulDB entry created
CNA	2025-08-28T13:05:52.000Z	VulDB entry last update

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