ELOG configuration file authorization bypass

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

Summary

CVE	CVE-2025-64348
State	PUBLISHED
Assigner	cisa-cg
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-31 19:15:51 UTC
Updated	2026-04-26 19:26:45 UTC
Description	ELOG allows an authenticated user to modify or overwrite the configuration file, resulting in denial of service. If the execute

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from 9119a7d8-5eab-497f-8521-727c672e3725

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

EPSS: 0.001190000 probability, percentile 0.304610000 (date 2026-04-26)

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
4.0	9119a7d8-5eab-497f-8521-727c672e3725	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/V
4.0	CNA	DECLARED	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/V
3.1	9119a7d8-5eab-497f-8521-727c672e3725	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H
3.1	CNA	DECLARED	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elog Project	Elog	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ELOG	ELOG	affected *	Not specified

CNA	ELOG	ELOG	affected	Not specified

References

Reference	Source
www.cve.org/CVERecord	9119a7d8-5eab-497f-8521-727c672e3725
bitbucket.org/ritt/elog/commits/f81e5695c40997322fe2713bfdeba459d9de09dc	9119a7d8-5eab-497f-8521-727c672e3725
bitbucket.org/ritt/elog/commits/7092ff64f6eb9521f8cc8c52272a020bf3730946	9119a7d8-5eab-497f-8521-727c672e3725
raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2025/va-25-304-01.json	9119a7d8-5eab-497f-8521-727c672e3725
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Karl Meister, CISA (en)

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