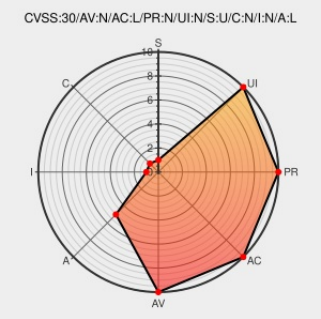
CVE-2020-8859

Published on: 03/23/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:59 PM UTC

CVE-2020-8859

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Electronic Logbook from Psi contain the following vulnerability:

This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of ELOG Electronic Logbook 3.1.4-283534d. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of HTTP parameters. A crafted request can trigger the dereference of a null pointer. An attacker can leverage this vulnerability to create a denial-of-service condition. Was ZDI-CAN-10115.

CVE-2020-8859 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **ELOG** - **Electronic Logbook** version **3.1.4-283534d**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
	Vendor Advisory elog.psi.ch application/octet-stream	MISC elog.psi.ch/elogs/Forum/69114
ZDI-20-252 | Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-20-252/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Psi	Electronic Logbook	3.1.4-283534d	All	All	All
Application	Psi	Electronic Logbook	3.1.4-283534d	All	All	All

cpe:2.3:a:psi:electronic_logbook:3.1.4-283534d:*:*:*:*:*:*:*:

cpe:2.3:a:psi:electronic_logbook:3.1.4-283534d:*:*:*:*:*:*:*:

Discovery Credit

Asif Akbar of Trend Micro Security Research

← Previous ID

Next ID→