



CVE-2006-0348

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

Summary

CVE	CVE-2006-0348
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-01-21 01:03:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Format string vulnerability in the write_logfile function in ELOG before 2.6.1 allows remote attackers to cause a denial of se

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

EPSS: 0.013440000 probability, percentile 0.800790000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

ntegrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Stefan Ritt	Elog Web Logbook	2.0.0	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.0.1	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.0.2	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.0.3	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.0.4	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.0.5	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.1.0	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.1.1	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.1.2	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.1.3	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.2.0	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.2.1	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.2.2	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.2.3	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.2.4	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.4	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.5	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.5.6	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.5.7	All	All	All
Application	Stefan Ritt	Elog Web Logbook	2.6.0	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference			Source	Link		
ELOG Web Logbook Multiple Remote Input Validation Vulnerabilities			af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			af854a3a-2127-422b-91ae-364da2661108	www.vupen.com		
ELOG Site			af854a3a-2127-422b-91ae-364da2661108	midas.psi.ch		
Secunia - Advisories - ELOG Multiple Security Issue and Vulnerabilities			af854a3a-2127-422b-91ae-364da2661108	secunia.com		
www.osvdb.org/22646			af854a3a-2127-422b-91ae-364da2661108	www.osvdb.org		
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcl		
Debian update for elog - Advisories - Secunia			af854a3a-2127-422b-91ae-364da2661108	secunia.com		
Debian -- Security Information -- DSA-967-1 elog			af854a3a-2127-422b-91ae-364da2661108	www.debian.org		
CVE Program record			CVE.ORG	www.cve.org		

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)