



CVE-2012-3815

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-3815
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-27 21:55:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	Buffer overflow in RunTime.exe in Sielco Sistemi Winlog Pro SCADA before 2.07.18 and Winlog Lite SCADA before 2.07.18

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sielcosistemi	Winlog Lite	2.06.00	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.03	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.04	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.06	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.09	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.10	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.12	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.13	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.14	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.18	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.21	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.24	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.25	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.28	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.40	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.46	All	All	All
Application	Sielcosistemi	Winlog Lite	2.06.50	All	All	All

[illegible]

Application	Sielcosistemi	Winlog Pro	2.06.24	All	All	All
Application	Sielcosistemi	Winlog Pro	2.06.25	All	All	All
Application	Sielcosistemi	Winlog Pro	2.06.28	All	All	All
Application	Sielcosistemi	Winlog Pro	2.06.40	All	All	All
Application	Sielcosistemi	Winlog Pro	2.06.46	All	All	All
Application	Sielcosistemi	Winlog Pro	2.06.50	All	All	All
Application	Sielcosistemi	Winlog Pro	2.06.60	All	All	All
Application	Sielcosistemi	Winlog Pro	2.06.73	All	All	All
Application	Sielcosistemi	Winlog Pro	2.06.86	All	All	All
Application	Sielcosistemi	Winlog Pro	2.07.00	All	All	All
Application	Sielcosistemi	Winlog Pro	2.07.01	All	All	All
Application	Sielcosistemi	Winlog Pro	2.07.08	All	All	All
Application	Sielcosistemi	Winlog Pro	2.07.09	All	All	All
Application	Sielcosistemi	Winlog Pro	2.07.11	All	All	All
Application	Sielcosistemi	Winlog Pro	All	All	All	All

References						
Reference				Source	Link	
Advisory / Exploit: Sielco Sistemi Winlog Buffer Overflow <= v2.07.16 [Update: 02.07.2012] www.s3cur1ty.de				MISC	www.s3cur1ty	
Security Alerts - Secunia				SECUNIA	secunia.com	
SCADA Software HMI SCADA systems WEB SCADA system				CONFIRM	www.sielcosis	
Winlog Lite Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker				SECTRAK	securitytracke	
20120605 Sielco Sistemi Winlog Buffer Overflow <= v2.07.14				BUGTRAQ	archives.neoh	
IBM X-Force Exchange				XF	exchange.xfor	
Sielco Sistemi Winlog Lite Buffer Overflow Vulnerability				BID	www.securityf	
82654				OSVDB	www.osvdb.or	
SCADA Software HMI SCADA systems WEB SCADA system				CONFIRM	www.sielcosis	
404 - File Not Found CISA				MISC	www.us-cert.g	
CVE Program record				CVE.ORG	www.cve.org	
NVD vulnerability detail				NVD	nvd.nist.gov	

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](#)