CVE-2011-0517

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

Summary

CVE	CVE-2011-0517
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-20 19:00:12 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Stack-based buffer overflow in Sielco Sistemi Winlog Pro 2.07.00 and earlier, when Run TCP/IP server is enabled, allows re

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sielcosistemi	Winlog Pro	All	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
US-CERT Vulnerability Note VU#496040 - Sielco Sistemi Winlog server stack overflow	af854a3a-2127-422b-91ae-364da2661108	www.k
Winlog Pro TCP/IP Server Buffer Overflow Vulnerability - Secunia.com	af854a3a-2127-422b-91ae-364da2661108	secuni
Winlog Pro Malformed Packet Stack Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.s
Sielco Sistemi Winlog <= 2.07.00 Stack Overflow	af854a3a-2127-422b-91ae-364da2661108	www.e
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchar
Sielco Sistemi Winlog Buffer Overflow - SecurityReason.com	af854a3a-2127-422b-91ae-364da2661108	securit
aluigi.org/adv/winlog_1-adv.txt	af854a3a-2127-422b-91ae-364da2661108	aluigi.c
404 - File Not Found | CISA	af854a3a-2127-422b-91ae-364da2661108	www.u
osvdb.org/70418	af854a3a-2127-422b-91ae-364da2661108	osvdb.
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	www.v
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

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