CVE-2003-1160

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

Summary

CVE	CVE-2003-1160
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-10-30 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	FlexWATCH Network video server 132 allows remote attackers to bypass authentication and gain administrative privileges

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Seyeon	Flexwatch Network Video Server	2.2	All	All	All

Application	Seyeon	Flexwatch Network Video Server	model_132	All	All	All

Vendor Declared Affected Products

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

References

Reference	So
SecurityTracker.com Archives - FlexWATCH Network Video Server Authentication Flaw Grants Administrative Access to Remote Users	af8
packetstormsecurity.nl/0310-exploits/FlexWATCH.txt	af8
Secunia - Advisories - FlexWATCH Network Video Server User Authentication Bypass Vulnerability	af8
IBM X-Force Exchange	af8
www.osvdb.org/2842	af8
Seyeon FlexWATCH Network Video Server Unauthorized Administrative Access Vulnerability	af8
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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