



CVE-2015-0929

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

Summary

CVE	CVE-2015-0929
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-03 22:59:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	time.htm in the web interface on SerVision HVG Video Gateway devices with firmware before 2.2.26a78 allows remote atta

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: CWE-284 | 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
Hardware	Servision	Hvg400	-	All	All	All

Operating System	Servision	Hvg Video Gateway Firmware	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		
Vulnerability Note VU#522460 - SerVision HVG Video Gateway web interface contains multiple vulnerabilities				af854a3a-2127-422b-91ae-36		
CVE Program record				CVE.ORG		
NVD vulnerability detail				NVD		
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						