CVE-2015-2903

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

Summary

CVE	CVE-2015-2903
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-04 03:59:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The CWSAPI SOAP service in HP ArcSight SmartConnectors before 7.1.6 has a hardcoded password, which makes it easi

Risk And Classification

Primary CVSS: v2.0 6.9 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/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	Hp	Arcsight Smartconnectors	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
Vulnerability Note VU#350508 - HP ArcSight SmartConnector fails to properly validate SSL and contains a hard-coded password
HP ArcSight SmartConnectors Default Password and Lack of Certificate Validation Let Remote Users Gain Access to the Target System or M
Document Display | HPE Support Center
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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