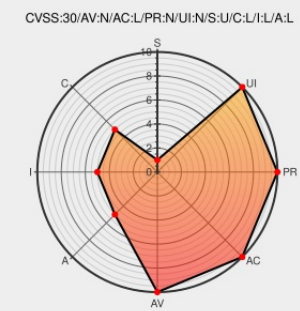
CVE-2015-6863

Published on: 01/15/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

CVE-2015-6863

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Arcsight Logger from Hp contain the following vulnerability:

HPE ArcSight Logger before 6.1P1 allows remote attackers to execute arbitrary code via unspecified input to the (1) Intellicus or (2) client-certificate upload component.

CVE-2015-6863 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.3 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	LOW

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Document Display | HPE Support Center	Patch, Vendor Advisory, h20566.www2.hpe.com, text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04941487

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Arcsight Logger	All	All	All	All

cpe:2.3:a:hp:arcsight_logger:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report