CVE-2016-4379

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-4379
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-08 16:59:00 UTC
Updated	2016-11-28 20:17:00 UTC
Description	The TLS implementation in HPE Integrated Lights-Out 3 (aka iLO3) firmware before 1.88 does not properly use a MAC prot

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Hp	Integrated Lights-out 3	-	All	All	All
Hardware	Hp	Integrated Lights-out 3	-	All	All	All
Operating System	Hp	Integrated Lights-out 3 Firmware	All	All	All	All

References

Reference
HP Integrated Lights-Out CVE-2016-4379 Information Disclosure Vulnerability
HPE integrated Lights Out (iLO) TLS CBC Mode Attack Lets Remote Users Obtain Potentially Sensitive Information on the Target System - Se
www.iacr.org/archive/eurocrypt2002/23320530/cbc02_e02d.pdf
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.