CVE-2016-4396

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

Summary

CVE	CVE-2016-4396
State	PUBLISHED
Assigner	hpe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-28 21:59:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	HPE System Management Homepage before v7.6 allows remote attackers to have an unspecified impact via unknown vect

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

EPSS: 0.014570000 probability, percentile 0.809590000 (date 2026-05-09)

Problem Types: CWE-119 | Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
2.0	nvd@nist.gov	Primary	7.8		AV:N/AC:L/Au:N/C:N/I:C/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Complete

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	System Management Homepage	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platfc
CNA	HPE	HPE System Management Homepage Before V7.6	affected HPE System Management Homepage before v7.6	Not sp

References

Reference	Source
Zero Day Initiative	af854a3a-2127-4
HP System Management Homepage Multiple Security Vulnerabilities	af854a3a-2127-4
Document Display | HPE Support Center	af854a3a-2127-4
[R1] HP System Management Homepage (SMH) Multiple Remote Stack Buffer Overflows - Research Advisory | Tenable®	af854a3a-2127-4
HPE Support document - HPE Support Center	af854a3a-2127-4
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.

Free CVE JSON API cve.report/api

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