CVE-2011-1867

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

Summary

CVE	CVE-2011-1867
State	PUBLISHED
Assigner	hp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-07-11 20:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Stack-based buffer overflow in iNodeMngChecker.exe in the User Access Manager (UAM) 5.0 before SP1 E0101P03 and E

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-119 | 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
Application	Hp	Endpoint Admission Defense	5.0	All	All	All

Application	Hp	Endpoint Admission Defense	5.0	e0101	All	All
Application	Hp	Intelligent Management Center	All	All	All	All
Application	Hp	User Access Manager	5.0	All	All	All
Application	Hp	User Access Manager	5.0	e0101	All	All

Vendor Declared Affected Products

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

References

Reference	Source
HP Intelligent Management Center UAM - SecurityReason.com	af854a3a-2
IBM X-Force Exchange	af854a3a-2
www.osvdb.org/73597	af854a3a-2
HP Intelligent Management Centre Products 'iNodeMngChecker.exe' Remote Code Execution Vulnerability	af854a3a-2
SecurityFocus	af854a3a-2
'[security bulletin] HPSB3C02687 SSRT100377 rev.1 - HP Intelligent Management Center User Access Mana' - MARC	af854a3a-2
HP Intelligent Management Center Products Packet Handling Buffer Overflow Vulnerability - Secunia.com	af854a3a-2
Zero Day Initiative	af854a3a-2
SecurityTracker: HP Intelligent Management Center UAM and EAD Buffer Overflow Lets Remote Users Execute Arbitrary Code	af854a3a-2
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.