CVE-2010-1039

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2010-1039
State	PUBLIC
Assigner	hp-security-alert@hp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-05-20 17:30:00 UTC
Updated	2018-10-10 19:55:00 UTC
Description	Format string vulnerability in the _msgout function in rpc.pcnfsd in IBM AIX 6.1, 5.3, and earlier; IBM VIOS 2.1, 1.5, and ear

Risk And Classification

Problem Types: CWE-134

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Hp-ux	b.11.11	All	All	All
Operating System	Hp	Hp-ux	b.11.23	All	All	All
Operating System	Hp	Hp-ux	b.11.31	All	All	All
Operating System	Hp	Hp-ux	b.11.11	All	All	All
Operating System	Hp	Hp-ux	b.11.23	All	All	All
Operating System	Hp	Hp-ux	b.11.31	All	All	All
Application	Hp	Nfs/oncplus	All	All	All	All
Application	Hp	Nfs/oncplus	All	All	All	All
Operating System	Ibm	Aix	1.2.1	All	All	All
Operating System	Ibm	Aix	1.3	All	All	All
Operating System	Ibm	Aix	2.2.1	All	All	All
Operating System	Ibm	Aix	3.1	All	All	All
Operating System	Ibm	Aix	3.2	All	All	All
Operating System	Ibm	Aix	3.2.0	All	All	All
Operating System	Ibm	Aix	3.2.4	All	All	All
Operating System	Ibm	Aix	3.2.5	All	All	All
Operating System	Ibm	Aix	4	All	All	All

Operating System	Ibm	Aix	4.0	All	All	All
Operating System	Ibm	Aix	4.1	All	All	All
Operating System	Ibm	Aix	4.1.1	All	All	All
Operating System	Ibm	Aix	4.1.2	All	All	All
Operating System	Ibm	Aix	4.1.3	All	All	All
Operating System	Ibm	Aix	4.1.4	All	All	All
Operating System	Ibm	Aix	4.1.5	All	All	All
Operating System	Ibm	Aix	4.2	All	All	All
Operating System	Ibm	Aix	4.2.0	All	All	All
Operating System	Ibm	Aix	4.2.1	All	All	All
Operating System	Ibm	Aix	4.2.1.12	All	All	All
Operating System	Ibm	Aix	4.3	All	All	All
Operating System	Ibm	Aix	4.3.0	All	All	All
Operating System	Ibm	Aix	4.3.1	All	All	All
Operating System	Ibm	Aix	4.3.2	All	All	All
Operating System	Ibm	Aix	4.3.3	All	All	All
Operating System	Ibm	Aix	430	All	All	All
Operating System	Ibm	Aix	5.1	All	All	All
Operating System	Ibm	Aix	5.1.0.10	All	All	All
Operating System	Ibm	Aix	5.1l	All	All	All
Operating System	Ibm	Aix	5.2	All	All	All
Operating System	Ibm	Aix	5.2.0	All	All	All
Operating System	Ibm	Aix	5.2.0.50	All	All	All
Operating System	Ibm	Aix	5.2.0.54	All	All	All
Operating System	Ibm	Aix	5.2.2	All	All	All
Operating System	Ibm	Aix	5.2_l	All	All	All
Operating System	Ibm	Aix	6.1	All	All	All
Operating System	Ibm	Aix	1.2.1	All	All	All
Operating System	Ibm	Aix	1.3	All	All	All
Operating System	Ibm	Aix	2.2.1	All	All	All
Operating System	Ibm	Aix	3.1	All	All	All
Operating System	Ibm	Aix	3.2	All	All	All
Operating System	Ibm	Aix	3.2.0	All	All	All
Operating System	Ibm	Aix	3.2.4	All	All	All
Operating System	Ibm	Aix	3.2.5	All	All	All

Operating System	Ibm	Aix	4	All	All	All
Operating System	Ibm	Aix	4.0	All	All	All
Operating System	Ibm	Aix	4.1	All	All	All
Operating System	Ibm	Aix	4.1.1	All	All	All
Operating System	Ibm	Aix	4.1.2	All	All	All
Operating System	Ibm	Aix	4.1.3	All	All	All
Operating System	Ibm	Aix	4.1.4	All	All	All
Operating System	Ibm	Aix	4.1.5	All	All	All
Operating System	Ibm	Aix	4.2	All	All	All
Operating System	Ibm	Aix	4.2.0	All	All	All
Operating System	Ibm	Aix	4.2.1	All	All	All
Operating System	Ibm	Aix	4.2.1.12	All	All	All
Operating System	Ibm	Aix	4.3	All	All	All
Operating System	Ibm	Aix	4.3.0	All	All	All
Operating System	Ibm	Aix	4.3.1	All	All	All
Operating System	Ibm	Aix	4.3.2	All	All	All
Operating System	Ibm	Aix	4.3.3	All	All	All
Operating System	Ibm	Aix	430	All	All	All
Operating System	Ibm	Aix	5.1	All	All	All
Operating System	Ibm	Aix	5.1.0.10	All	All	All
Operating System	Ibm	Aix	5.1l	All	All	All
Operating System	Ibm	Aix	5.2	All	All	All
Operating System	Ibm	Aix	5.2.0	All	All	All
Operating System	Ibm	Aix	5.2.0.50	All	All	All
Operating System	Ibm	Aix	5.2.0.54	All	All	All
Operating System	Ibm	Aix	5.2.2	All	All	All
Operating System	Ibm	Aix	5.2_l	All	All	All
Operating System	Ibm	Aix	6.1	All	All	All
Operating System	Ibm	Aix	All	All	All	All
Application	Ibm	Vios	1.4	All	All	All
Application	Ibm	Vios	2.1	All	All	All
Application	Ibm	Vios	1.4	All	All	All
Application	Ibm	Vios	2.1	All	All	All
Application	Ibm	Vios	All	All	All	All
Operating System	Sgi	Irix	6.5	All	All	All

Operating System	Sgi	Irix	6.5	All	All	All

References

Reference	Source
IBM - My notifications	CONFIRM
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
IBM X-Force Exchange	XF
Repository / Oval Repository	OVAL
Update Protection against Multiple Vendors rpc.pcnfsd Syslog Format String Vulnerability	MISC
IZ73599: POTENTIAL SECURITY ISSUE. APPLIES TO AIX 6100-05	AIXAPAR
Repository / Oval Repository	OVAL
Multiple Vendor 'rpc.pcnfsd' Integer Overflow Vulnerability	BID
aix.software.ibm.com/aix/efixes/security/pcnfsd_advisory.asc	CONFIRM
IZ73590: POTENTIAL SECURITY ISSUE. APPLIES TO AIX 5300-12	AIXAPAR
HP-UX NFS/ONCplus Integer Overflow Vulnerability - Advisories - Community	SECUNIA
IZ75465: POTENTIAL SECURITY ISSUE. APPLIES TO AIX 6100-02	AIXAPAR
SecurityTracker.com Archives - IBM AIX Integer Overflow in rpc.pcnfsd Lets Remote Users Execute Arbitrary Code	SECTRACK
IZ75440: POTENTIAL SECURITY ISSUE. APPLIES TO AIX 6100-03	AIXAPAR
64729	OSVDB
SecurityTracker.com Archives - HP-UX Integer Overflow in ONCPlus 'rpc.pcnfsd' Lets Remote Users Execute Arbitrary Code	SECTRACK
'[security bulletin] HPSBUX02523 SSRT100036 rev.1 - HP-UX Running ONCPlus, Remote Denial of Service (' - MARC	HP
IZ75369: POTENTIAL SECURITY ISSUE. APPLIES TO AIX 6100-04	AIXAPAR
IZ73874: POTENTIAL SECURITY ISSUE. APPLIES TO AIX 5300-09	AIXAPAR
SecurityFocus	BUGTRAQ
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
IZ73681: POTENTIAL SECURITY ISSUE. APPLIES TO AIX 5300-11	AIXAPAR
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
IZ73757: POTENTIAL SECURITY ISSUE. APPLIES TO AIX 5300-10	AIXAPAR
IBM AIX "rpc.pcnfsd" Format String Vulnerability - Advisories - Community	SECUNIA
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.