CVE-2003-0724

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2003-0724
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-10-20 04:00:00 UTC
Updated	2008-09-05 20:35:00 UTC
Description	ssh on HP Tru64 UNIX 5.1B and 5.1A does not properly handle RSA signatures when digital certificates and RSA keys are

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Compaq	Tru64	5.1a	All	All	All
Operating System	Compaq	Tru64	5.1a_pk1_bl1	All	All	All
Operating System	Compaq	Tru64	5.1a_pk2_bl2	All	All	All
Operating System	Compaq	Tru64	5.1a_pk3_bl3	All	All	All
Operating System	Compaq	Tru64	5.1a_pk4_bl21	All	All	All
Operating System	Compaq	Tru64	5.1a_pk5_bl23	All	All	All
Operating System	Compaq	Tru64	5.1b_pk2_bl22	All	All	All
Operating System	Compaq	Tru64	5.1a	All	All	All
Operating System	Compaq	Tru64	5.1a_pk1_bl1	All	All	All
Operating System	Compaq	Tru64	5.1a_pk2_bl2	All	All	All
Operating System	Compaq	Tru64	5.1a_pk3_bl3	All	All	All
Operating System	Compaq	Tru64	5.1a_pk4_bl21	All	All	All
Operating System	Compaq	Tru64	5.1a_pk5_bl23	All	All	All
Operating System	Compaq	Tru64	5.1b_pk2_bl22	All	All	All

References

Reference	Source	Link	Tags

SSRT3588	HP	www.securityfocus.com	Vendor Advisory
HP Tru64 SSH Undisclosed RSA Key Potential Authentication Bypass Vulnerability	BID	www.securityfocus.com	Patch, Vendor A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.