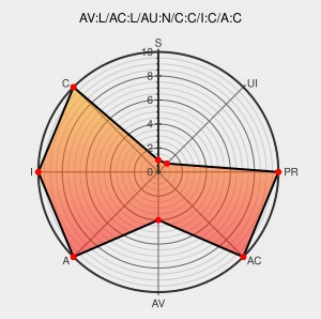
CVE-2002-1616

Published on: 08/01/2002 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1616

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tru64 from Hp contain the following vulnerability:

Multiple buffer overflows in HP Tru64 UNIX 5.1a, 5.1, 5.0a, 4.0g, and 4.0f allow local users to gain root privileges via (1) su, (2) chsh, (3) passwd, (4) chfn, (5) dxchpwd, and (6) libc.

CVE-2002-1616 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Tru64 CHFN Local Privilege Escalation Vulnerability	Patch, cve.report (archive), text/html	BID 5381
CERT/CC Vulnerability Note VU#177067	Third Party Advisory, US Government Resource, www.kb.cert.org, text/html	CERT-VN VU#177067
CERT Vulnerability Notes Database	US Government Resource, www.kb.cert.org, text/html, Inactive Link, Not Archived	CERT-VN VU#864083
CERT/CC Vulnerability Note VU#671627	Third Party Advisory, US Government Resource, www.kb.cert.org	CERT-VN VU#671627

	text/html	
	Exploit www.blacksheepnetworks.com text/x-perl	MISC www.blacksheepnetworks.com/security/hack/tru64/TRU64_su.txt
CERT/CC Vulnerability Note VU#137555	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#137555
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF tru64-chfn-bo(10614)
Neohapsis Archives - Compaq Tru64 - [Bulletin] SSRT2257 HP Tru64 UNIX /usr/bin/su buffer overflow potential exploit - From Rich.Boren_at_hp.com	web.archive.org text/html Inactive Link Not Archived	HP SSRT2259
SecurityFocus	Vendor Advisory www.securityfocus.com text/html	BUGTRAQ 20020902 Happy Labor Day from Snosoft
Tru64 CHSH Local Privilege Escalation Vulnerability	Vendor Advisory cve.report (archive) text/html	BID 5379
No Description Provided	archives.neohapsis.com Inactive Link Not Archived	FULLDISC 20020919 iDEFENSE OSF1/Tru64 3.x vuln clarification
Tru64 DXCHPWD Local Privilege Escalation Vulnerability	Patch cve.report (archive) text/html	BID 5382
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF tru64-dxchpwd-bo(11620)
Tru64 passwd Local Privilege Escalation Vulnerability	Patch cve.report (archive) text/html	BID 5380
CERT/CC Vulnerability Note VU#193347	Patch US Government Resource www.kb.cert.org text/html	CERT-VN VU#193347

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Tru64	4.0f	All	All	All
Operating System	Hp	Tru64	4.0g	All	All	All

Operating System	Hp	Tru64	5.0a	All	All	All
Operating System	Hp	Tru64	5.1	All	All	All
Operating System	Hp	Tru64	5.1af	All	All	All
Operating System	Hp	Tru64	4.0f	All	All	All
Operating System	Hp	Tru64	4.0g	All	All	All
Operating System	Hp	Tru64	5.0a	All	All	All
Operating System	Hp	Tru64	5.1	All	All	All
Operating System	Hp	Tru64	5.1af	All	All	All

cpe:2.3:o:hp:tru64:4.0f:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:4.0g:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.0a:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1af:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:4.0f:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:4.0g:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.0a:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1af:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→