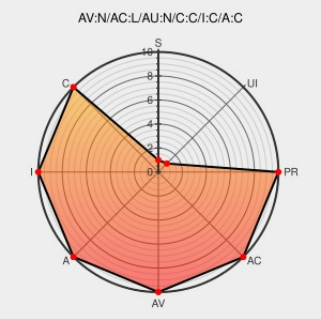
CVE-2003-1496

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-1496

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



Certain versions of Tru64 from Hp contain the following vulnerability:

Unspecified vulnerability in CDE dtmailpr of HP Tru64 4.0F through 5.1B allows local users to gain privileges via unknown attack vectors. NOTE: due to lack of details in the vendor advisory, it is not clear whether this is the same issue as CVE-1999-0840.

CVE-2003-1496 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
Secunia - Advisories - HP Tru64 Unix dtmailpr Privilege Escalation Vulnerability	web.archive.org text/html	SECUNIA 9990
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF tru64-dtmailpr-gain-privileges(13418)
HP Tru64 CDE dtmailpr Unspecified Privileged Access Vulnerability	cve.report (archive) text/html	BID 8813
SecurityFocus HOME Advisories: Tru64 UNIX Potential Security Vulnerability with d	web.archive.org text/html Inactive Link Not Archived	COMPAQ SSRT3589

comment@cve.report.

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	4.0f_pk6_bl17	All	All	All
Operating System	Hp	Tru64	4.0f_pk7_bl18	All	All	All
Operating System	Hp	Tru64	4.0f_pk8_bl22	All	All	All
Operating System	Hp	Tru64	4.0g	All	All	All
Operating System	Hp	Tru64	4.0g_pk3_bl17	All	All	All
Operating System	Hp	Tru64	4.0g_pk4_bl22	All	All	All
Operating System	Hp	Tru64	5.1	All	All	All
Operating System	Hp	Tru64	5.1a	All	All	All
Operating System	Hp	Tru64	5.1a_pk1_bl1	All	All	All
Operating System	Hp	Tru64	5.1a_pk2_bl2	All	All	All
Operating System	Hp	Tru64	5.1a_pk3_bl3	All	All	All
Operating System	Hp	Tru64	5.1a_pk4_bl21	All	All	All
Operating System	Hp	Tru64	5.1a_pk5_bl23	All	All	All
Operating System	Hp	Tru64	5.1b	All	All	All
Operating System	Hp	Tru64	5.1_pk3_bl17	All	All	All
Operating System	Hp	Tru64	5.1_pk4_bl18	All	All	All
Operating System	Hp	Tru64	5.1_pk5_bl19	All	All	All
Operating System	Hp	Tru64	5.1_pk6_bl20	All	All	All
Operating	Hp	Tru64	4.0f	All	All	All

Operating System	Hp	Tru64	4.0f	All	All	All
Operating System	Hp	Tru64	4.0f_pk6_bl17	All	All	All
Operating System	Hp	Tru64	4.0f_pk7_bl18	All	All	All
Operating System	Hp	Tru64	4.0f_pk8_bl22	All	All	All
Operating System	Hp	Tru64	4.0g	All	All	All
Operating System	Hp	Tru64	4.0g_pk3_bl17	All	All	All
Operating System	Hp	Tru64	4.0g_pk4_bl22	All	All	All
Operating System	Hp	Tru64	5.1	All	All	All
Operating System	Hp	Tru64	5.1a	All	All	All
Operating System	Hp	Tru64	5.1a_pk1_bl1	All	All	All
Operating System	Hp	Tru64	5.1a_pk2_bl2	All	All	All
Operating System	Hp	Tru64	5.1a_pk3_bl3	All	All	All
Operating System	Hp	Tru64	5.1a_pk4_bl21	All	All	All
Operating System	Hp	Tru64	5.1a_pk5_bl23	All	All	All
Operating System	Hp	Tru64	5.1b	All	All	All
Operating System	Hp	Tru64	5.1_pk3_bl17	All	All	All
Operating System	Hp	Tru64	5.1_pk4_bl18	All	All	All
Operating System	Hp	Tru64	5.1_pk5_bl19	All	All	All
Operating System	Hp	Tru64	5.1_pk6_bl20	All	All	All

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

cpe:2.3:o:hp:tru64:4.0f_pk6_bl17:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:4.0f_pk7_bl18:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:4.0f_pk8_bl22:*:*:*:*:*:*:*:

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

cpe:2.3:o:hp:tru64:4.0g_pk3_bl17:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:4.0g_pk4_bl22:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:hp:tru64:5.1a_pk1_bl1:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1a_pk2_bl2:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1a_pk3_bl3:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1a_pk4_bl21:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1a_pk5_bl23:*:*:*:*:*:*:*:

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

cpe:2.3:o:hp:tru64:5.1_pk3_bl17:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1_pk4_bl18:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1_pk5_bl19:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1_pk6_bl20:*:*:*:*:*:*:*:

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

cpe:2.3:o:hp:tru64:4.0f_pk6_bl17:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:4.0f_pk7_bl18:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:4.0f_pk8_bl22:*:*:*:*:*:*:*:

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

cpe:2.3:o:hp:tru64:4.0g_pk3_bl17:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:4.0g_pk4_bl22:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:hp:tru64:5.1a_pk1_bl1:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1a_pk2_bl2:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1a_pk3_bl3:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1a_pk4_bl21:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1a_pk5_bl23:*:*:*:*:*:*:*:

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

cpe:2.3:o:hp:tru64:5.1_pk3_bl17:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1_pk4_bl18:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1_pk5_bl19:*:*:*:*:*:*:*:

cpe:2.3:o:hp:tru64:5.1_pk6_bl20:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→