



CVE-2006-5452

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2006-5452
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-10-23 17:07:00 UTC
Updated	2018-10-17 21:42:00 UTC
Description	Buffer overflow in dtmail on HP Tru64 UNIX 4.0F through 5.1B and HP-UX B.11.00 through B.11.23 allows local users to e

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Hp-ux	11.00	All	All	All
Operating System	Hp	Hp-ux	11.11	All	All	All
Operating System	Hp	Hp-ux	11.22	All	All	All
Operating System	Hp	Hp-ux	11.23	All	ia64_64-bit	All
Operating System	Hp	Hp-ux	11.4	All	All	All
Operating System	Hp	Hp-ux	11.00	All	All	All
Operating System	Hp	Hp-ux	11.11	All	All	All
Operating System	Hp	Hp-ux	11.22	All	All	All
Operating System	Hp	Hp-ux	11.23	All	ia64_64-bit	All
Operating System	Hp	Hp-ux	11.4	All	All	All
Operating System	Hp	Tru64	4.0f	All	All	All
Operating System	Hp	Tru64	4.0f	pk8	All	All
Operating System	Hp	Tru64	4.0g	All	All	All
Operating System	Hp	Tru64	4.0g	pk4	All	All
Operating System	Hp	Tru64	5.0a	All	All	All
Operating System	Hp	Tru64	5.1	All	All	All
Operating System	Hp	Tru64	5.1a	All	All	All

Operating System	Hp	Tru64	5.1a	pk6	All	All
Operating System	Hp	Tru64	5.1af	All	All	All
Operating System	Hp	Tru64	5.1b	pk1	All	All
Operating System	Hp	Tru64	5.1b2	pk4	All	All
Operating System	Hp	Tru64	5.1b3	All	All	All
Operating System	Hp	Tru64	4.0f	All	All	All
Operating System	Hp	Tru64	4.0f	pk8	All	All
Operating System	Hp	Tru64	4.0g	All	All	All
Operating System	Hp	Tru64	4.0g	pk4	All	All
Operating System	Hp	Tru64	5.0a	All	All	All
Operating System	Hp	Tru64	5.1	All	All	All
Operating System	Hp	Tru64	5.1a	All	All	All
Operating System	Hp	Tru64	5.1a	pk6	All	All
Operating System	Hp	Tru64	5.1af	All	All	All
Operating System	Hp	Tru64	5.1b	pk1	All	All
Operating System	Hp	Tru64	5.1b2	pk4	All	All
Operating System	Hp	Tru64	5.1b3	All	All	All

References						
Reference						Solution
Repository / Oval Repository						OVAL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUI
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUI
SecurityTracker.com Archives - HP UNIX Dtm ail Buffer Overflow Lets Local Users Gain Root Privileges						SEC
IBM X-Force Exchange						XF
Netragard - Penetration Testing, Red Teaming & App Testing Company						MIS
SecurityTracker.com Archives - (HP Issues Fix for Tru64 UNIX) HP UNIX Dtm ail Buffer Overflow Lets Local Users Gain Root Privileges						SEC
SecurityTracker.com Archives - (HP Issues Fix for HP-UX) HP UNIX Dtm ail Buffer Overflow Lets Local Users Gain Root Privileges						SEC
HP Tru64 Unix dtmail Privilege Escalation Vulnerability - Advisories - Secunia						SEC
HPSBUX02162						HP
HP DTMail Attachment Argument Buffer Overflow Vulnerability						BID
HP-UX dtmail Privilege Escalation Vulnerability - Advisories - Secunia						SEC
SecurityFocus						HP
CVE Program record						CVI
NVD vulnerability detail						NVI

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)