



Published on: 08/30/2002 04:00:00 AM UTC

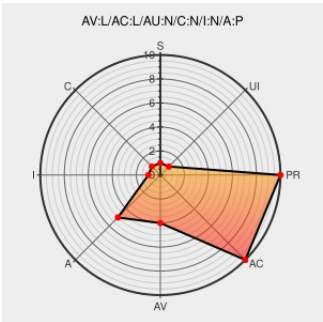
Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1610

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Hp-ux](#) from [Hp](#) contain the following vulnerability:

Unknown vulnerability in ping in HP Tru64 UNIX 5.1a, 5.1, 5.0a, 4.0g, and 4.0f allows local users to cause a denial of service.

CVE-2002-1610 has been assigned by  cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
HP Tru64 UNIX Multiple Local and Remote Buffer Overflow Vulnerabilities	cve.report (archive) text/html	 BID 5599
CERT/CC Vulnerability Note VU#612833	Third Party Advisory US Government Resource www.kb.cert.org text/html	 CERT-VN VU#612833
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF tru64- ping- dos(10014)
[security bulletin] SSRT2275 HP Tru64 UNIX - Potential BufferOverflows & SSRT2229 Potential Denial of Service (fwd)	Patch web.archive.org text/html Inactive Link Not Archived	 HP SSRT2229

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to 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	Hp-ux	10.20	All	All	All
Operating System	Hp	Hp-ux	11.00	All	All	All
Operating System	Hp	Hp-ux	11.04	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	10.20	All	All	All
Operating System	Hp	Hp-ux	11.00	All	All	All
Operating System	Hp	Hp-ux	11.04	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	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	5.1a	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	5.1a	All	All	All
cpe:2.3:o:hp:hp-ux:10.20:*****:						
cpe:2.3:o:hp:hp-ux:11.00:*****:						
cpe:2.3:o:hp:hp-ux:11.04:*****:						
cpe:2.3:o:hp:hp-ux:11.11:*****:						
cpe:2.3:o:hp:hp-ux:11.22:*****:						
cpe:2.3:o:hp:hp-ux:10.20:*****:						
cpe:2.3:o:hp:hp-ux:11.00:*****:						
cpe:2.3:o:hp:hp-ux:11.04:*****:						
cpe:2.3:o:hp:hp-ux:11.11:*****:						
cpe:2.3:o:hp:hp-ux:11.22:*****:						
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:tru64:5.1a:*****:						
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:tru64:5.1a:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#).

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