



CVE-2003-1097

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

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

CVE-2003-1097

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Buffer overflow in rexec on HP-UX B.10.20, B.11.00, and B.11.04, when setuid root, may allow local users to gain privileges via a long -l option.

CVE-2003-1097 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

N-088: Hewlett-Packard rexec Command Security Vulnerability

[Patch](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CIAC N-088](#)

No Description Provided

[Exploit](#)
[archives.neohapsis.com](#)
[Inactive Link](#) [Not Archived](#)

[BUGTRAQ 20030429 HP-UX rexec buffer overflow vulnerability](#)

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

[OVAL oval:org.mitre.oval:def:5611](#)

HP-UX RExec Remote Username Flag Local Buffer Overrun Vulnerability

[Exploit](#)
[Patch](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 7459](#)

CERT/CC Vulnerability Note VU#322540	text/html Third Party Advisory US Government Resource www.kb.cert.org text/html	 CERT-VN VU#322540
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF hp-rexec-command-bo(11890)
Hewlett-Packard Company Information for VU#322540	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	 HP HPSBUX0304-257

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	10.10	All	All	All
Operating System	Hp	Hp-ux	10.16	All	All	All
Operating System	Hp	Hp-ux	10.20	All	All	All
Operating System	Hp	Hp-ux	10.24	All	All	All
Operating System	Hp	Hp-ux	10.26	All	All	All
Operating System	Hp	Hp-ux	10.30	All	All	All
Operating System	Hp	Hp-ux	10.34	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	11.20	All	All	All
Operating System	Hp	Hp-ux	11.22	All	All	All
Operating System	Hp	Hp-ux	10.10	All	All	All

Operating System	Hp	Hp-ux	10.16	All	All	All
Operating System	Hp	Hp-ux	10.20	All	All	All
Operating System	Hp	Hp-ux	10.24	All	All	All
Operating System	Hp	Hp-ux	10.26	All	All	All
Operating System	Hp	Hp-ux	10.30	All	All	All
Operating System	Hp	Hp-ux	10.34	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	11.20	All	All	All
Operating System	Hp	Hp-ux	11.22	All	All	All
cpe:2.3:o:hp:hp-ux:10.10:*****:						
cpe:2.3:o:hp:hp-ux:10.16:*****:						
cpe:2.3:o:hp:hp-ux:10.20:*****:						
cpe:2.3:o:hp:hp-ux:10.24:*****:						
cpe:2.3:o:hp:hp-ux:10.26:*****:						
cpe:2.3:o:hp:hp-ux:10.30:*****:						
cpe:2.3:o:hp:hp-ux:10.34:*****:						
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:11.20:*****:						
cpe:2.3:o:hp:hp-ux:11.22:*****:						
cpe:2.3:o:hp:hp-ux:10.10:*****:						
cpe:2.3:o:hp:hp-ux:10.16:*****:						
cpe:2.3:o:hp:hp-ux:10.20:*****:						

cpe:2.3:o:hp:hp-ux:10.24:*****:
cpe:2.3:o:hp:hp-ux:10.26:*****:
cpe:2.3:o:hp:hp-ux:10.30:*****:
cpe:2.3:o:hp:hp-ux:10.34:*****:
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:11.20:*****:
cpe:2.3:o:hp:hp-ux:11.22:*****:

No vendor comments have been submitted for this CVE

← Previous IDNext ID →