

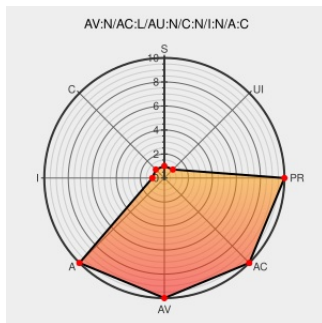


CVE-2005-3670

Published on: 11/18/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

CVE-2005-3670

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

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

Multiple unspecified vulnerabilities in the Internet Key Exchange version 1 (IKEv1) implementation in HP HP-UX B.11.00, B.11.11, and B.11.23 running IPsec, HP Jetdirect 635n IPv6/IPsec Print Server, and HP Tru64 UNIX 5.1B-3 and 5.1B-2/PK4, allow remote attackers to cause a denial of service via certain IKE packets, as demonstrated by the PROTON ISAKMP Test Suite for IKEv1. NOTE: due to the lack of

details in the HP advisory, it is unclear which of CVE-2005-3666, CVE-2005-3667, and/or CVE-2005-3668 this issue applies to.

CVE-2005-3670 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

No Description Provided

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

[MISC](#)
www.ee.oulu.fi/research/ouspg/protos/testing/c09/isakmp/

Secunia - Advisories - HP Tru64 UNIX
IPSEC/ISAKMP Processing Denial of Service

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 19174](#)

No Description Provided

www2.itrc.hp.com

[HP SSRT050979](#)

Inactive Link Not Archived

Secunia - Advisories - HP JetDirect Print Server
IPSec Denial of Service

Vendor Advisory
web.archive.org
text/html

 SECUNIA 17598

SecurityTracker.com Archives - HP JetDirect 635n
Print Server IKE Processing Lets Remote Users
Deny Service

Patch
securitytracker.com
text/html

 SECTrack 1015227

NISCC-273756: ISAKMP プロトコルの実装に複数
の脆弱性

Patch
jvn.jp
text/html

 MISC jvn.jp/niscc/NISCC-273756/index.html

Repository / Oval Repository

oval.cisecurity.org
text/html

 OVAL oval:org.mitre.oval:def:5642

Webmail : Solution de messagerie professionnelle -
OVHcloud- OVH

Vendor Advisory
www.vupen.com
text/html

 VUPEN ADV-2006-0880

SecurityTracker.com Archives - HP-UX IPSec IKE
Processing Lets Remote Users Deny Service

Patch
securitytracker.com
text/html

 SECTrack 1015229

HP-UX IKE Exchange Denial Of Service
Vulnerabilities

cve.report (archive)
text/html

 BID 15474

Webmail : Solution de messagerie professionnelle -
OVHcloud- OVH

Vendor Advisory
www.vupen.com
text/html

 VUPEN ADV-2005-2462

HP Jetdirect 635n IPv6/IPsec Print Server IKE
Exchange Denial Of Service Vulnerability

cve.report (archive)
text/html

 BID 15471

www.niscc.gov.uk
application/pdf

Inactive Link Not Archived

 MISC www.niscc.gov.uk/niscc/docs/re-20051114-01014.pdf?lang=en

Hewlett-Packard Company Information for
VU#226364

US Government Resource
www.kb.cert.org
text/html

 HP HPSBPI02078

SecurityTracker.com Archives - HP Tru64 UNIX
IPSec IKE Processing Lets Remote Users Deny
Service

Patch
securitytracker.com
text/html

 SECTrack 1015727

US-CERT Vulnerability Note VU#226364

Patch
US Government Resource
www.kb.cert.org
text/html

 CERT-VN VU#226364

HP Tru64 IKE Exchange Denial Of Service
Vulnerabilities

cve.report (archive)
text/html

 BID 17030

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	11.00	All	All	All
Operating System	Hp	Hp-ux	11.11	All	All	All
Operating System	Hp	Hp-ux	11.23	All	ia64_64-bit	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	11.23	All	ia64_64-bit	All
Hardware 	Hp	Jetdirect 635n	All	All	All	All
Hardware 	Hp	Jetdirect 635n	All	All	All	All
Operating System	Hp	Tru64	5.1b1	pk4	All	All
Operating System	Hp	Tru64	5.1b3	All	All	All
Operating System	Hp	Tru64	5.1b1	pk4	All	All
Operating System	Hp	Tru64	5.1b3	All	All	All
cpe:2.3:o:hp:hp-ux:11.00:*:*:*:*:*:						
cpe:2.3:o:hp:hp-ux:11.11:*:*:*:*:*:						
cpe:2.3:o:hp:hp-ux:11.23:*:ia64_64-bit:*:*:*:*:						
cpe:2.3:o:hp:hp-ux:11.00:*:*:*:*:*:						
cpe:2.3:o:hp:hp-ux:11.11:*:*:*:*:*:						
cpe:2.3:o:hp:hp-ux:11.23:*:ia64_64-bit:*:*:*:*:						
cpe:2.3:h:hp:jetdirect_635n:*:*:*:*:*:						
cpe:2.3:h:hp:jetdirect_635n:*:*:*:*:*:						
cpe:2.3:o:hp:tru64:5.1b1:pk4:*:*:*:*:*:						
cpe:2.3:o:hp:tru64:5.1b3:*:*:*:*:*:						
cpe:2.3:o:hp:tru64:5.1b1:pk4:*:*:*:*:*:						
cpe:2.3:o:hp:tru64:5.1b3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

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](#).

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