



# CVE-2005-4178

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

## Summary

<b>CVE</b>	CVE-2005-4178
<b>State</b>	PUBLIC
<b>Assigner</b>	security@debian.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-12-12 21:03:00 UTC
<b>Updated</b>	2018-10-30 16:28:00 UTC
<b>Description</b>	Buffer overflow in Dropbear server before 0.47 allows authenticated users to execute arbitrary code via unspecified inputs t

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	Debian Linux	3.0	All	All	All
Operating System	<a href="#">Debian</a>	Debian Linux	3.1	All	All	All
Operating System	<a href="#">Debian</a>	Debian Linux	3.0	All	All	All
Operating System	<a href="#">Debian</a>	Debian Linux	3.1	All	All	All
Application	<a href="#">Dropbear Ssh Project</a>	Dropbear Ssh	All	All	All	All
Application	<a href="#">Dropbear Ssh Project</a>	Dropbear Ssh	All	All	All	All

## References

Reference	Source	Link	Tags
Secunia - Advisories - Dropbear SSH Server Buffer Overflow Vulnerability	SECUNIA	<a href="#">secunia.com</a>	Third Party Advisory
Dropbear SSH Server Remote Buffer Overflow Vulnerability	BID	<a href="#">www.securityfocus.com</a>	Third Party Advisory, VDB
Dropbear SSH server and client	MISC	<a href="#">matt.ucc.asn.au</a>	Patch, Vendor Advisory
Secunia - Advisories - Debian update for dropbear	SECUNIA	<a href="#">secunia.com</a>	Third Party Advisory
Gentoo update for dropbear - Advisories - Secunia	SECUNIA	<a href="#">secunia.com</a>	Third Party Advisory
Gentoo Linux Documentation -- Dropbear: Privilege escalation	GENTOO	<a href="#">www.gentoo.org</a>	Third Party Advisory
Webmail   OVH- OVH	VUPEN	<a href="#">www.vupen.com</a>	Third Party Advisory
Dropbear 0.47 (and security fix)	MLIST	<a href="#">lists.ucc.gu.uwa.edu.au</a>	Patch, Vendor Advisory

Debian -- Security Information -- DSA-923-1 dropbear	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third Party Advisory
Dropbear SSH Server Remote Buffer Overflow Vulnerability	MITRE	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)