



# CVE-2012-0212

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

## Summary

<b>CVE</b>	CVE-2012-0212
<b>State</b>	PUBLIC
<b>Assigner</b>	security@debian.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-06-16 00:55:00 UTC
<b>Updated</b>	2023-11-07 02:09:00 UTC
<b>Description</b>	debdiff.pl in devscripts 2.10.x before 2.10.69 and 2.11.x before 2.11.4 allows remote attackers to execute arbitrary code via

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.0	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.1	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.10	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.11	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.12	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.13	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.14	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.15	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.16	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.17	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.18	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.18.1	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.19	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.20	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.21	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.22	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.23	All	All	All







Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.6	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.60	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.61	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.62	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.63	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.64	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.65.1	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.66	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.67	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.68	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.7	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.8	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.10.9	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.11.0	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.11.1	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.11.2	All	All	All
Application	<a href="#">Devscripts Devel Team</a>	<a href="#">Devscripts</a>	2.11.3	All	All	All

## References

Reference	Source	Link	Tags
Debian devscripts 'debdiff' Multiple Remote Code Execution Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
79322	OSVDB	<a href="http://www.osvdb.org">www.osvdb.org</a>	
USN-1593-1: devscripts vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	
Security Advisory SA47955 - Debian update for devscripts - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Vendor Advisory
USN-1366-1: devscripts vulnerabilities   Ubuntu	UBUNTU	<a href="http://ubuntu.com">ubuntu.com</a>	
404 Not Found		<a href="http://anonscm.debian.org">anonscm.debian.org</a>	
404 Not Found	CONFIRM	<a href="http://anonscm.debian.org">anonscm.debian.org</a>	
Security Advisory SA48039 - Ubuntu update for devscripts - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Vendor Advisory
Debian -- Security Information -- DSA-2409-1 devscripts	DEBIAN	<a href="http://www.debian.org">www.debian.org</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](#) 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](#).

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