



CVE-2006-3251

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

Summary

CVE	CVE-2006-3251
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-27 18:05:00 UTC
Updated	2017-07-20 01:32:00 UTC
Description	Heap-based buffer overflow in the array_push function in hashcash.c for Hashcash before 1.21 might allow attackers to ex

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hashcash	Hashcash	1.00	All	All	All
Application	Hashcash	Hashcash	1.01	All	All	All
Application	Hashcash	Hashcash	1.02	All	All	All
Application	Hashcash	Hashcash	1.03	All	All	All
Application	Hashcash	Hashcash	1.04	All	All	All
Application	Hashcash	Hashcash	1.05	All	All	All
Application	Hashcash	Hashcash	1.06	All	All	All
Application	Hashcash	Hashcash	1.07	All	All	All
Application	Hashcash	Hashcash	1.08	All	All	All
Application	Hashcash	Hashcash	1.09	All	All	All
Application	Hashcash	Hashcash	1.10	All	All	All
Application	Hashcash	Hashcash	1.11	All	All	All
Application	Hashcash	Hashcash	1.12	All	All	All
Application	Hashcash	Hashcash	1.13	All	All	All
Application	Hashcash	Hashcash	1.14	All	All	All
Application	Hashcash	Hashcash	1.15	All	All	All
Application	Hashcash	Hashcash	1.16	All	All	All

Application	Hashcash	Hashcash	1.17	All	All	All
Application	Hashcash	Hashcash	1.18	All	All	All
Application	Hashcash	Hashcash	1.19	All	All	All
Application	Hashcash	Hashcash	1.00	All	All	All
Application	Hashcash	Hashcash	1.01	All	All	All
Application	Hashcash	Hashcash	1.02	All	All	All
Application	Hashcash	Hashcash	1.03	All	All	All
Application	Hashcash	Hashcash	1.04	All	All	All
Application	Hashcash	Hashcash	1.05	All	All	All
Application	Hashcash	Hashcash	1.06	All	All	All
Application	Hashcash	Hashcash	1.07	All	All	All
Application	Hashcash	Hashcash	1.08	All	All	All
Application	Hashcash	Hashcash	1.09	All	All	All
Application	Hashcash	Hashcash	1.10	All	All	All
Application	Hashcash	Hashcash	1.11	All	All	All
Application	Hashcash	Hashcash	1.12	All	All	All
Application	Hashcash	Hashcash	1.13	All	All	All
Application	Hashcash	Hashcash	1.14	All	All	All
Application	Hashcash	Hashcash	1.15	All	All	All
Application	Hashcash	Hashcash	1.16	All	All	All
Application	Hashcash	Hashcash	1.17	All	All	All
Application	Hashcash	Hashcash	1.18	All	All	All
Application	Hashcash	Hashcash	1.19	All	All	All
Application	Hashcash	Hashcash	All	All	All	All

References						
Reference			Source	Link		Tags
Secunia - Advisories - Gentoo update for hashcash			SECUNIA	secunia.com		Vendor Advisory
Debian update for hashcash - Advisories - Secunia			SECUNIA	secunia.com		Vendor Advisory
Hashcash "array_push" Buffer Overflow Vulnerability - Advisories - Secunia			SECUNIA	secunia.com		Vendor Advisory
Gentoo Linux Documentation -- Hashcash: Possible heap overflow			GENTOO	www.gentoo.org		
www.hashcash.org/source/CHANGELOG			CONFIRM	www.hashcash.org		
Debian -- Security Information -- DSA-1114-1 hashcash			DEBIAN	www.debian.org		
Hashcash Remote Heap Buffer Overflow Vulnerability			BID	www.securityfocus.com		Patch
IBM X-Force Exchange			XF	exchange.xforce.ibmcloud.com		
Hashcash.org - Hashcash: A Distributed Denial of Service (DDoS) Mitigation System			VULNER	www.hashcash.org		Vendor Advisory

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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](#).

Free CVE JSON API cve.report/api

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