



CVE-2012-6620

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

Summary

CVE	CVE-2012-6620
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-16 21:55:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the (1) tasks and (2) search views in Horde Kronolith H4 before 3.0.17 a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Horde	Kronolith H4	3.0	All	All	All
Application	Horde	Kronolith H4	3.0	alpha1	All	All
Application	Horde	Kronolith H4	3.0	beta1	All	All
Application	Horde	Kronolith H4	3.0	rc1	All	All
Application	Horde	Kronolith H4	3.0	rc2	All	All
Application	Horde	Kronolith H4	3.0.1	All	All	All
Application	Horde	Kronolith H4	3.0.10	All	All	All
Application	Horde	Kronolith H4	3.0.11	All	All	All
Application	Horde	Kronolith H4	3.0.12	All	All	All
Application	Horde	Kronolith H4	3.0.13	All	All	All
Application	Horde	Kronolith H4	3.0.14	All	All	All
Application	Horde	Kronolith H4	3.0.15	All	All	All
Application	Horde	Kronolith H4	3.0.2	All	All	All
Application	Horde	Kronolith H4	3.0.3	All	All	All
Application	Horde	Kronolith H4	3.0.4	All	All	All
Application	Horde	Kronolith H4	3.0.5	All	All	All
Application	Horde	Kronolith H4	3.0.6	All	All	All

Application	Horde	Kronolith H4	3.0.7	All	All	All
Application	Horde	Kronolith H4	3.0.8	All	All	All
Application	Horde	Kronolith H4	3.0.9	All	All	All
Application	Horde	Kronolith H4	3.0	All	All	All
Application	Horde	Kronolith H4	3.0	alpha1	All	All
Application	Horde	Kronolith H4	3.0	beta1	All	All
Application	Horde	Kronolith H4	3.0	rc1	All	All
Application	Horde	Kronolith H4	3.0	rc2	All	All
Application	Horde	Kronolith H4	3.0.1	All	All	All
Application	Horde	Kronolith H4	3.0.10	All	All	All
Application	Horde	Kronolith H4	3.0.11	All	All	All
Application	Horde	Kronolith H4	3.0.12	All	All	All
Application	Horde	Kronolith H4	3.0.13	All	All	All
Application	Horde	Kronolith H4	3.0.14	All	All	All
Application	Horde	Kronolith H4	3.0.15	All	All	All
Application	Horde	Kronolith H4	3.0.2	All	All	All
Application	Horde	Kronolith H4	3.0.3	All	All	All
Application	Horde	Kronolith H4	3.0.4	All	All	All
Application	Horde	Kronolith H4	3.0.5	All	All	All
Application	Horde	Kronolith H4	3.0.6	All	All	All
Application	Horde	Kronolith H4	3.0.7	All	All	All
Application	Horde	Kronolith H4	3.0.8	All	All	All
Application	Horde	Kronolith H4	3.0.9	All	All	All
Application	Horde	Kronolith H4	All	All	All	All

References						
Reference	Source	Link	Tags			
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com				
[announce] Kronolith H4 (3.0.17) (final)	MLIST	lists.horde.org				
Tickets :: [#11189] XSS vulnerability in Tasks view	MISC	bugs.horde.org				
Horde Kronolith Multiple Cross Site Scripting Vulnerabilities	BID	www.securityfocus.com				
Escape content (Bug #11189). · horde/horde@1228a68 · GitHub	CONFIRM	github.com	Exploit, Patch			
Security Alerts - Secunia	SECUNIA	secunia.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](#)