



# CVE-2005-4189

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2005-4189
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-12-13 11:03:00 UTC
<b>Updated</b>	2011-03-08 02:27:00 UTC
<b>Description</b>	Multiple cross-site scripting (XSS) vulnerabilities in Horde Kronolith H3 before 2.0.6 allow remote authenticated users to inj

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Horde	Kronolith H3	2.0	All	All	All
Application	Horde	Kronolith H3	2.0.1	All	All	All
Application	Horde	Kronolith H3	2.0.2	All	All	All
Application	Horde	Kronolith H3	2.0.2_rc1	All	All	All
Application	Horde	Kronolith H3	2.0.3	All	All	All
Application	Horde	Kronolith H3	2.0.3_rc1	All	All	All
Application	Horde	Kronolith H3	2.0.4	All	All	All
Application	Horde	Kronolith H3	2.0.4_rc1	All	All	All
Application	Horde	Kronolith H3	2.0.5	All	All	All
Application	Horde	Kronolith H3	2.0_alpha	All	All	All
Application	Horde	Kronolith H3	2.0_beta	All	All	All
Application	Horde	Kronolith H3	2.0_rc1	All	All	All
Application	Horde	Kronolith H3	2.0_rc2	All	All	All
Application	Horde	Kronolith H3	2.0_rc3	All	All	All
Application	Horde	Kronolith H3	2.0	All	All	All
Application	Horde	Kronolith H3	2.0.1	All	All	All
Application	Horde	Kronolith H3	2.0.2	All	All	All

Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0.2_rc1	All	All	All
Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0.3	All	All	All
Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0.3_rc1	All	All	All
Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0.4	All	All	All
Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0.4_rc1	All	All	All
Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0.5	All	All	All
Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0_alpha	All	All	All
Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0_beta	All	All	All
Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0_rc1	All	All	All
Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0_rc2	All	All	All
Application	<a href="#">Horde</a>	<a href="#">Kronolith H3</a>	2.0_rc3	All	All	All

## References

### Reference

21608

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

21610

[404 - Page not found! - SEC Consult](#)

[Horde Kronolith Multiple HTML Injection Vulnerabilities](#)

[Debian -- Security Information -- DSA-970-1 kronolith](#)

[Neohapsis Archives - Full Disclosure List - #0459 - \[Full-disclosure\] SEC Consult SA-20051211-0 :: Several XSS issues in Horde Framework,](#)

[Debian update for kronolith - Advisories - Secunia](#)

[Secunia - Advisories - Kronolith Script Insertion Vulnerabilities](#)

21609

[\[announce\] Kronolith H3 \(2.0.6\) \(final\)](#)

21611

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

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

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](#)**