



# CVE-2008-5071

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2008-5071
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-11-14 18:07:59 UTC
<b>Updated</b>	2026-04-23 00:35:47 UTC
<b>Description</b>	Multiple eval injection vulnerabilities in itpm_estimate.php in Yoxel 1.23beta and earlier allow remote authenticated users to

## Risk And Classification

**Primary CVSS:** v2.0 9 from nvd@nist.gov

AV:N/AC:L/Au:S/C:C/I:C/A:C

**Problem Types:** CWE-94 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yoxel	Yoxel	1.06beta	All	All	All

Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.07beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.08beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.09beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.10beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.11beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.12beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.13beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.14beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.15beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.16beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.17beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.18beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.19beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.20	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.20beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.21	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.21beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.22	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	1.22beta	All	All	All
Application	<a href="#">Yoxel</a>	<a href="#">Yoxel</a>	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

#### References

Reference	Source	Link
Yoxel 'itpm_estimate.php' Multiple PHP Code Injection Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.se...</a>
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	<a href="#">exchang...</a>
CXSecurity - IDS	af854a3a-2127-422b-91ae-364da2661108	<a href="#">securityr...</a>
Yoxel 1.23beta - 'itpm_estimate.php' Remote Code Execution - PHP webapps Exploit	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.ex...</a>
CVE Program record	CVE.ORG	<a href="#">www.cve...</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist...</a>

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](#)