



# CVE-2011-0401

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2011-0401                                                                                                               |
| <b>State</b>           | PUBLISHED                                                                                                                   |
| <b>Assigner</b>        | mitre                                                                                                                       |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2011-01-10 20:00:17 UTC                                                                                                     |
| <b>Updated</b>         | 2026-04-29 01:13:23 UTC                                                                                                     |
| <b>Description</b>     | Piwik before 1.1 does not properly limit the number of files stored under tmp/sessions/, which might allow remote attackers |

## Risk And Classification

**Primary CVSS:** v2.0 5 from nvd@nist.gov

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

**Problem Types:** CWE-264 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

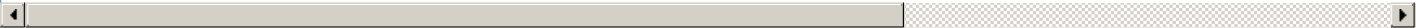
## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Matomo | Matomo  | 0.1     | All    | All     | All      |

|             |                        |                        |        |     |     |     |
|-------------|------------------------|------------------------|--------|-----|-----|-----|
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.1.1  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.1.10 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.1.2  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.1.3  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.1.4  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.1.5  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.1.6  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.1.7  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.1.8  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.1.9  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.1  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.10 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.11 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.12 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.13 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.14 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.16 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.17 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.18 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.19 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.2  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.20 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.22 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.23 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.24 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.25 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.26 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.27 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.28 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.29 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.3  | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.30 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.31 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.32 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.33 | All | All | All |
| Application | <a href="#">Matomo</a> | <a href="#">Matomo</a> | 0.2.34 | All | All | All |



| Reference                                                                                                  | Source                     |
|------------------------------------------------------------------------------------------------------------|----------------------------|
| osvdb.org/70381                                                                                            | af854a3a-2127-422b-91ae-36 |
| Piwik Prior to 1.1 Multiple Security Vulnerabilities                                                       | af854a3a-2127-422b-91ae-36 |
| #1279 (Custom ("user") session handler using database (ie MySQL) instead of "files") – Piwik Web Analytics | af854a3a-2127-422b-91ae-36 |
| IBM X-Force Exchange                                                                                       | af854a3a-2127-422b-91ae-36 |
| Piwik 1.1 - Piwik                                                                                          | af854a3a-2127-422b-91ae-36 |
| #1910 (Check session.gc_probability so tmp/sessions files don't grow out of control) – Piwik Web Analytics | af854a3a-2127-422b-91ae-36 |
| CVE Program record                                                                                         | CVE.ORG                    |
| NVD vulnerability detail                                                                                   | NVD                        |



No vendor comments have been submitted for this CVE.

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