



# CVE-2006-0571

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2006-0571                                                                                                                    |
| State           | PUBLISHED                                                                                                                        |
| Assigner        | mitre                                                                                                                            |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                     |
| Published       | 2006-02-07 18:06:00 UTC                                                                                                          |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                          |
| Description     | Multiple cross-site scripting (XSS) vulnerabilities in phpstatus 1.0 allow remote attackers to inject arbitrary web script or HT |

## Risk And Classification

**Primary CVSS:** v2.0 4.3 from nvd@nist.gov

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

**EPSS:** 0.005270000 probability, percentile 0.671470000 (date 2026-04-16)

**Problem Types:** NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------|--------|---------|---------|--------|---------|----------|
|------|--------|---------|---------|--------|---------|----------|

|                                                                      |               |           |                                      |                                                                  |     |     |
|----------------------------------------------------------------------|---------------|-----------|--------------------------------------|------------------------------------------------------------------|-----|-----|
| Application                                                          | Hinton Design | Phpstatus | 1.0                                  | 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                                                             |     |     |
| PHPStatus Multiple Input Validation Vulnerabilities                  |               |           | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.securityfocus.com">www.securityfocus.com</a> |     |     |
| phpstatus Authentication Bypass - CXSecurity.com                     |               |           | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://securityreason.com">securityreason.com</a>       |     |     |
| PHPStatus Multiple Vulnerabilities - Advisories - Secunia            |               |           | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://secunia.com">secunia.com</a>                     |     |     |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH     |               |           | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.vupen.com">www.vupen.com</a>                 |     |     |
| SecurityFocus                                                        |               |           | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.securityfocus.com">www.securityfocus.com</a> |     |     |
| eVuln.com - phpstatus Authentication Bypass                          |               |           | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://evuln.com">evuln.com</a>                         |     |     |
| CVE Program record                                                   |               |           | CVE.ORG                              | <a href="http://www.cve.org">www.cve.org</a>                     |     |     |
| NVD vulnerability detail                                             |               |           | NVD                                  | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                   |     |     |
| <div><div></div><div></div></div>                                    |               |           |                                      |                                                                  |     |     |
| No vendor comments have been submitted for this CVE.                 |               |           |                                      |                                                                  |     |     |
| There are currently no legacy QID mappings associated with this CVE. |               |           |                                      |                                                                  |     |     |