



# CVE-2006-0910

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

## Summary

|                 |                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2006-0910                                                                                                                           |
| State           | PUBLISHED                                                                                                                               |
| Assigner        | mitre                                                                                                                                   |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                            |
| Published       | 2006-02-28 11:02:00 UTC                                                                                                                 |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                                 |
| Description     | Invision Power Board (IPB) 2.1.4 and earlier allows remote attackers to list directory contents via a direct request to multiple files. |

## Risk And Classification

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

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

EPSS: 0.006280000 probability, percentile 0.702790000 (date 2026-04-16)

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

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

## NVD Known Affected Configurations (CPE 2.3)

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

|             |                                         |                                      |           |     |     |     |
|-------------|-----------------------------------------|--------------------------------------|-----------|-----|-----|-----|
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.0.0     | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.0.1     | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.0.2     | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.0.3     | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.0.4     | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.1.0     | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.1.1     | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.1.2     | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.1.3     | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.1.4     | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.1_beta2 | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.1_beta3 | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.1_beta4 | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.1_beta5 | All | All | All |
| Application | <a href="#">Invision Power Services</a> | <a href="#">Invision Power Board</a> | 2.1_rc1   | All | All | All |

| Vendor Declared Affected Products |        |         |              |               |
|-----------------------------------|--------|---------|--------------|---------------|
| Source                            | Vendor | Product | Version      | Platforms     |
| CNA                               | Na     | N/a     | affected n/a | Not specified |

| References                                                                                                  |                             |
|-------------------------------------------------------------------------------------------------------------|-----------------------------|
| Reference                                                                                                   | Source                      |
| Neo Security Team - Security Researchers - Advisories - Invision Power Board 2.1.4 Multiple Vulnerabilities | af854a3a-2127-422b-91ae-364 |
| Neo Security Team - Security Researchers - Advisories - Invision Power Board 2.1.4 Multiple Vulnerabilities | af854a3a-2127-422b-91ae-364 |
| IBM X-Force Exchange                                                                                        | af854a3a-2127-422b-91ae-364 |
| SecurityFocus                                                                                               | af854a3a-2127-422b-91ae-364 |
| 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.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)