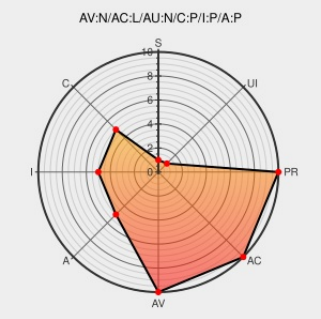
# CVE-2006-1551

Published on: 04/13/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

## CVE-2006-1551

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Pajax from Georges Auberger contain the following vulnerability:

Eval injection vulnerability in pajax_call_dispatcher.php in PAJAX 0.5.1 and earlier allows remote attackers to execute arbitrary code via the (1) $method and (2) $args parameters.

CVE-2006-1551 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 7.5 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| No Description Provided | www.osvdb.org<br>Inactive Link Not Archived | OSVDB 24618 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | www.vupen.com<br>text/html | VUPEN ADV-2006-1353 |
| PAJAX Arbitrary Code Execution Vulnerabilities - Advisories - Secunia | web.archive.org<br>text/html | SECUNIA 19653 |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com<br>text/html | XF pajax-pajaxcalldispatcher-code-execution(25859) |
| PAJAX Multiple Arbitrary PHP Code Execution Vulnerabilities | cve.report (archive)<br>text/html | BID 17519 |
| RedTeam Pentesting - PAJAX Remote Code Injection and File | Exploit | MISC www.redteam- |

| | | |
|---|---|---|
| Inclusion Vulnerability | Vendor Advisory<br>web.archive.org<br>text/xml<br>Inactive Link Not Archived | pentesting.de/advisories/rt-sa-2006-001.php |
| SecurityFocus | www.securityfocus.com<br>text/html | BUGTRAQ 20060413 PAJAX Remote Code Injection and File Inclusion Vulnerability |
| Neohapsis Archives - Full Disclosure List - #0270 - [Full-disclosure] PAJAX Remote Code Injection and File Inclusion Vulnerability | web.archive.org<br>text/html<br>Inactive Link Not Archived | FULLDISC 20060413 PAJAX Remote file inclusion and File Inclusion Vulnerability |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Georges Auberger | Pajax | 0.5.0 | All | All | All |
| Application | Georges Auberger | Pajax | 0.5.1 | All | All | All |
| Application | Georges Auberger | Pajax | 0.5.0 | All | All | All |
| Application | Georges Auberger | Pajax | 0.5.1 | All | All | All |

cpe:2.3:a:georges_auberger:pajax:0.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:georges_auberger:pajax:0.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:georges_auberger:pajax:0.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:georges_auberger:pajax:0.5.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→