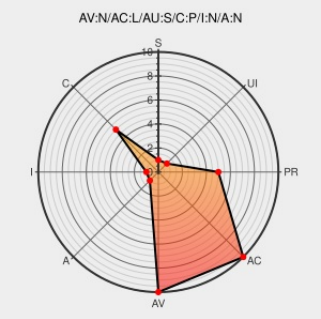
# CVE-2004-2616

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 11/07/2023 01:57:00 AM UTC

## CVE-2004-2616

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




Certain versions of Activepost Standard from Onnuri Infotek contain the following vulnerability:

The file server in ActivePost Standard 3.1 and earlier allows remote authenticated users to obtain sensitive information by uploading a file, which reveals the path in a success message.

CVE-2004-2616 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 4 - MEDIUM

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

### CVE References

| Description | Tags | Link |
|---|---|---|
| | Exploit, Vendor Advisory, aluigi.altervista.org, text/plain | MISC aluigi.altervista.org/adv/actp-adv.txt |
| No Description Provided | www.osvdb.org, Inactive Link, Not Archived | OSVDB 10235 |
| SecurityTracker.com Archives - ActivePost Lets Remote Users Upload Arbitrary Files, Detemine Passwords, and Crash the System, and D | Exploit, Vendor Advisory, securitytracker.com, text/html | SECTRACK 1011406 |
| MARC: Mailing list ARChives | marc.info, text/html | 20040923 Multiple vulnerabilities in ActivePost Standard 3.1 |

| | | |
|---|---|---|
| 'Multiple vulnerabilities in ActivePost Standard 3.1' - MARC | marc.info<br>text/html | BUGTRAQ 20040923 Multiple vulnerabilities in ActivePost Standard 3.1 |
| Neohapsis Archives - Full Disclosure List - #0852 - [Full-Disclosure] Multiple vulnerabilities in ActivePost Standard 3.1 | Exploit<br>Vendor Advisory<br>web.archive.org<br>text/html<br>Inactive Link Not Archived | FULLDISC 20040923 Multiple vulnerabilities in ActivePost Standard 3.1 |

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 | Onnuri Infotek | Activepost Standard | 2.5 | All | All | All |
| Application | Onnuri Infotek | Activepost Standard | 3.0 | All | All | All |
| Application | Onnuri Infotek | Activepost Standard | 2.5 | All | All | All |
| Application | Onnuri Infotek | Activepost Standard | 3.0 | All | All | All |
| Application | Onnuri Infotek | Activepost Standard | All | All | All | All |

cpe:2.3:a:onnuri_infotek:activepost_standard:2.5:*:*:*:*:*:*:*:

cpe:2.3:a:onnuri_infotek:activepost_standard:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:onnuri_infotek:activepost_standard:2.5:*:*:*:*:*:*:*:

cpe:2.3:a:onnuri_infotek:activepost_standard:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:onnuri_infotek:activepost_standard:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→