



CVE-2007-1742

Published on: 04/13/2007 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:00:00 AM UTC

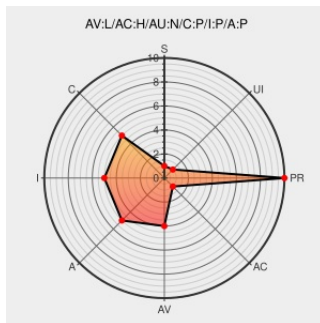
CVE-2007-1742

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Http Server](#) from [Apache](#) contain the following vulnerability:

suexec in Apache HTTP Server (httpd) 2.2.3 uses a partial comparison for verifying whether the current directory is within the document root, which might allow local users to perform unauthorized operations on incorrect directories, as demonstrated using "html_backup" and "htmleditor" under an "html" directory. NOTE: the researcher, who is

reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root."

CVE-2007-1742 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **3.7 - LOW**

Access Vector

LOCAL

Access Complexity

HIGH

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

No Description Provided

[osvdb.org](#)

[OSVDB 38640](#)

Inactive Link **Not Archived**

No Description Provided

[web.archive.org](#)

[text/html](#)

Inactive Link **Not Archived**

[IDEFENSE 20070411 Apache HTTPD suEXEC Multiple Vulnerabilities](#)

No Description Provided

[marc.info](#)

[text/html](#)

[MLIST \[apache-http-dev\] 20070328 \[Fwd: iDefense Final Notice \[IDEF1445\]\]](#)

Apache suEXEC Bugs May Let Local Users Gain Elevated

[www.securitytracker.com](#)

[SECTrack 1017904](#)

Privileges - SecurityTracker

text/html

'Re: [Fwd: iDefense Final Notice [IDEF1445]]' - MARC

marc.info

text/html

MLIST [apache-http-dev] 20070328

Re: [Fwd: iDefense Final Notice [IDEF1445]]

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	Apache	Http Server	2.2.3	All	All	All
Application	Apache	Http Server	2.2.3	All	All	All

cpe:2.3:a:apache:http_server:2.2.3:****:****:

cpe:2.3:a:apache:http_server:2.2.3:****:****:

← Previous ID

Next ID→