



CVE-2005-1344

Published on: 04/27/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1344

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Buffer overflow in htdigest in Apache 2.0.52 may allow attackers to execute arbitrary code via a long realm argument. NOTE: since htdigest is normally only locally accessible and not setuid or setgid, there are few attack vectors which would lead to an escalation of privileges, unless htdigest is executed from a CGI program. Therefore this may not be a vulnerability.

CVE-2005-1344 has been assigned by [M](#) 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
Luca Ercoli - IT Security Specialist	Exploit www.lucaercoli.it text/plain	# MISC www.lucaercoli.it/advs/htdigest.txt
Apache HTDigest Realm Command Line Argument Buffer Overflow Vulnerability	cve.report (archive) text/html	🌐 BID 13537
Resend: APPLE-SA-2005-05-03 Security Update 2005-005	lists.apple.com text/html	🍏 APPLE APPLE-SA-2005-05-03
No Description Provided	Exploit www.osvdb.org	🌐 OSVDB 12848

[Inactive Link](#) **Not Archived**

SecuriTeam.com TM - Apache "htdigest" Buffer Overflow	Exploit www.securiteam.com text/html	 MISC www.securiteam.com/unixfocus/5EP061FEKC.html
APPLE-SA-2005-08-17 Security Update 2005-007 v1.1	lists.apple.com text/html	 APPLE APPLE-SA-2005-08-17
APPLE-SA-2005-08-15 Security Update 2005-007	lists.apple.com text/html	 APPLE APPLE-SA-2005-08-15
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	2.0.52	All	All	All
Application	Apache	Http Server	2.0.52	All	All	All
cpe:2.3:a:apache:http_server:2.0.52:*****:						
cpe:2.3:a:apache:http_server:2.0.52:*****:						
← Previous ID Next ID →						