



Published on: 12/31/1999 05:00:00 AM UTC

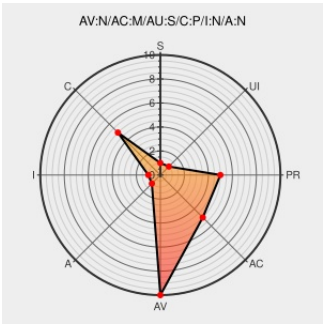
Last Modified on: 03/23/2021 11:27:32 PM UTC

CVE-1999-1590

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Wwwcount](#) from [Wwwcount](#) contain the following vulnerability:

Directory traversal vulnerability in Muhammad A. Muquit wwwcount (Count.cgi) 2.3 allows remote attackers to read arbitrary GIF files via "." sequences in the image parameter, a different vulnerability than CVE-1999-0021.

CVE-1999-1590 has been assigned by [M cve@mitre.org](mailto:m_cve@mitre.org) to track the vulnerability

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Bugtraq: Security flaw in Count.cgi (wwwcount)	Exploit Vendor Advisory seclists.org text/html	 BUGTRAQ 19971010 Security flaw in Count.cgi (wwwcount)

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)

Known/Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Wwwcount	Wwwcount	2.3	All	All	All
Application	Wwwcount	Wwwcount	2.3	All	All	All
cpe:2.3:a:wwwcount:wwwcount:2.3:*:*:*:*:*:						
cpe:2.3:a:wwwcount:wwwcount:2.3:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID →		