



CVE-2005-3594

Published on: 11/16/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

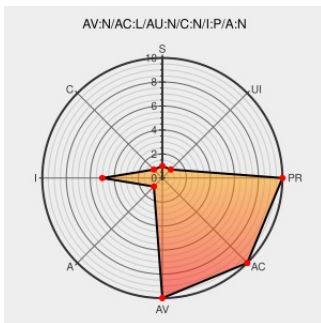
CVE-2005-3594

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [E107](#) from [E107](#) contain the following vulnerability: game_score.php in e107 allows remote attackers to insert high scores via HTTP POST methods utilizing the \$player_name, \$player_score, and \$game_name variables.

CVE-2005-3594 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

**Access
Vector**

NETWORK

**Access
Complexity**

LOW

Authentication

NONE

**Confidentiality
Impact**

NONE

**Integrity
Impact**

PARTIAL

**Availability
Impact**

NONE

CVE References

Description

Tags

Link

e107 Games System exploit - CXSecurity.com

[securityreason.com](#)
[text/html](#)

[SREASON 158](#)

'e107 Games System exploit' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20051107 e107 Games System exploit](#)

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	E107	E107	All	All	All	All
Application	E107	E107	All	All	All	All
cpe:2.3:a:e107:e107:*****:						
cpe:2.3:a:e107:e107:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		