



CVE-2008-7295

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2008-7295
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-08-09 19:55:00 UTC
Updated	2021-07-23 15:12:00 UTC
Description	Microsoft Internet Explorer cannot properly restrict modifications to cookies established in HTTPS sessions, which allows m

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Ie	All	All	All	All
Application	Microsoft	Ie	All	All	All	All
Application	Microsoft	Internet Explorer	All	All	All	All

References

Reference

Part2 - browsersec - Google Code - Browser Security Handbook, part 2
Security: Cookie forcing
...Application Security...: Cookie Forcing - Trust your cookies no more
Security: Some less obvious benefits of HSTS
660053 – (CVE-2011-2976) [SECURITY] If a BUGLIST cookie is compromised, it can be used to XSS show_bug.cgi and inject HTML into <he
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)