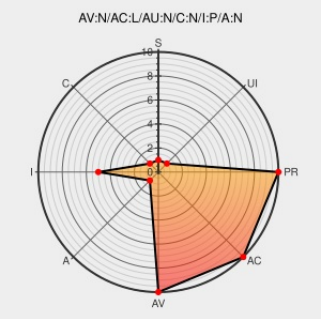
CVE-2004-1527

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 07/23/2021 12:55:00 PM UTC

CVE-2004-1527

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ie from Microsoft contain the following vulnerability:

Microsoft Internet Explorer 6.0 SP1 does not properly handle certain character strings in the Path attribute, which can cause it to modify cookies in other domains when the attacker's domain name is within the target's domain name or when wildcard DNS is being used, which allows remote attackers to hijack web sessions.

CVE-2004-1527 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
セキュリティ対策のラック｜情報を守るセキュリティ対策のパイオニア	Patch, Vendor Advisory, www.lac.co.jp, text/html	MISC www.lac.co.jp/business/sns/intelligence/SNSadvisory_e/79_e.html
Microsoft Internet Explorer Cookie Overwrite Vulnerability	cve.report (archive), text/html	BID 11680
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF ie-path-cookie-overwrite(18073)
Secunia - Advisories - Microsoft Internet Explorer Cookie Path Attribute Vulnerability	Patch, web.archive.org, text/html	SECUNIA 13208
'[SNS Advisory No.79] A Possibility of Cookie Overwrite in' - MARC	marc.info, text/html	BUGTRAQ 20041115 [SNS Advisory No.79] A Possibility of Cookie Overwrite in Microsoft Internet Explorer

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	Microsoft	Ie	6.0	All	All	All
Application	Microsoft	Ie	6.0	sp1	All	All
Application	Microsoft	Ie	6.0	All	All	All
Application	Microsoft	Ie	6.0	sp1	All	All
Application	Microsoft	Internet Explorer	6.0	All	All	All

cpe:2.3:a:microsoft:ie:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:ie:6.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:ie:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:ie:6.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:internet_explorer:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→