



CVE-2006-6986

Published on: 02/08/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:05 PM UTC

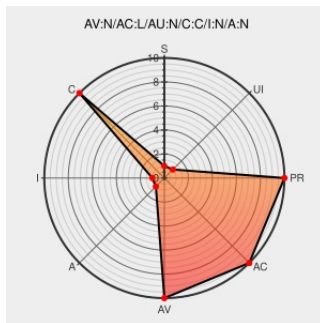
CVE-2006-6986

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Cross-domain vulnerability in PhaseOut 5.4.4 allows remote attackers to access restricted information from other domains via an object tag with a data parameter that references a link on the attacker's originating site that specifies a Location HTTP header that references the target site, which then makes that content available through the outerHTML attribute of the object, a similar vulnerability to CVE-2006-3280.

CVE-2006-6986 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

COMPLETE

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

- UNSECURED SYSTEMS -: Multiple Browsers Information Disclosure vuln.

[pridels0.blogspot.com](#)
[text/html](#)

[MISC pridels0.blogspot.com/2006/06/multiple-browsers-information.html](#)

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	Phaseout	Phaseout	5.4.4	All	All	All
Application	Phaseout	Phaseout	5.4.4	All	All	All
cpe:2.3:a:phaseout:phaseout:5.4.4:*****:						
cpe:2.3:a:phaseout:phaseout:5.4.4:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		