



CVE-2005-3634

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

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

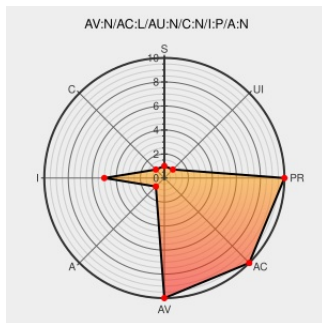
CVE-2005-3634

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Sap Web Application Server](#) from [Sap](#) contain the following vulnerability:

frameset.htm in the BSP runtime in SAP Web Application Server (WAS) 6.10 through 7.00 allows remote attackers to log users out and redirect them to arbitrary web sites via a close command in the sap-sessioncmd parameter and a URL in the sap-exiturl parameter.

CVE-2005-3634 has been assigned by [M](#) 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

[www.cybsec.com](#)
[application/pdf](#)

MISC
[www.cybsec.com/vuln/CYBSEC_Security_Advisory_Multiple_XSS_in_SAP_WAS.pdf](#)

No Description Provided

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

BUGTRAQ 20051109 CYBSEC - Security Advisory: Phishing Vector in SAP WAS

Phishing Vector in
SAP WAS -
CXSecurity.com

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

SREASON 163

SAP Web Application
Server Input
Validation Holes
Permit HTTP
Response Splitting,
Cross-Site Scripting,
and Phishing Attacks -

[Vendor Advisory](#)
[www.securitytracker.com](#)
[text/html](#)

SECTRAK 1015174

text/html



text/html



text/html



text/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	Sap	Sap Web Application Server	6.10	All	All	All
Application	Sap	Sap Web Application Server	6.20	All	All	All
Application	Sap	Sap Web Application Server	6.40	All	All	All
Application	Sap	Sap Web Application Server	7.0	All	All	All
Application	Sap	Sap Web Application Server	6.10	All	All	All
Application	Sap	Sap Web Application Server	6.20	All	All	All
Application	Sap	Sap Web Application Server	6.40	All	All	All
Application	Sap	Sap Web Application Server	7.0	All	All	All

```
cpe:2.3:a:sap:sap_web_application_server:6.10:*:*:*:*:*:
```

```
cpe:2.3:a:sap:sap_web_application_server:6.20:*:*:*:*:*.*
```

```
cpe:2.3:a:sap:sap web application server:6.40:::*:*:*:*.*
```

```
cpe:2.3:a:sap:sap web application server:7.0:*:*:*:*:*:*
```

```
cpe:2.3:a:sap:sap_web_application_server:6.10:*:*:*:*:*.*
```

```
cpe:2.3:a:sap:sap_web_application_server:6.20:*:*:*:*:*.*
```

```
cpe:2.3:a:sap:sap_web_application_server:6.40:*:*:*:*:*.*
```

cpe:2.3:a:sap:sap_web_application_server:7.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#)