



CVE-2005-3635

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

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

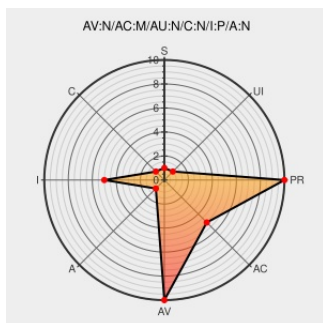
CVE-2005-3635

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

Multiple cross-site scripting (XSS) vulnerabilities in SAP Web Application Server (WAS) 6.10 through 7.00 allow remote attackers to inject arbitrary web script or HTML via (1) the sap-syscmd in sap-syscmd and (2) the BspApplication field in the SYSTEM PUBLIC test application.

CVE-2005-3635 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

IBM X-Force
Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
[text/html](#)

[XF sap-fameset-systempublic-xss\(23027\)](#)

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

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

SAP Web Application
Server Multiple Cross-
Site Scripting
Vulnerabilities

[Exploit](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 15361](#)

SAP Web Application
Server Input
Validation Holes
Permit HTTP

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

[SECTrack 1015174](#)

Response Splitting,
Cross-Site Scripting,
and Phishing Attacks -
SecurityTracker

No Description Provided

www.osvdb.org

OSVDB 20716

Inactive Link

Not Archived

Secunia - Advisories -
SAP Web Application
Server Multiple
Vulnerabilities

Vendor Advisory

web.archive.org

text/html

X SECUNIA 17515

No Description Provided

www.osvdb.org

OSVDB 20717

Inactive Link

Not Archived

No Description Provided

marc.info

text/html

BUGTRAQ 20051109 CYBSEC - Security Advisory: Multiple XSS in SAP WAS

Multiple XSS in SAP
WAS -
CXSecurity.com

securityreason.com

text/html

CX SREASON 162

Webmail : Solution de
messagerie
professionnelle -
OVHcloud- OVH

www.vupen.com

text/html

VUPEN ADV-2005-2361

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](#)