



CVE-2013-0571

Published on: 04/26/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:41 PM UTC

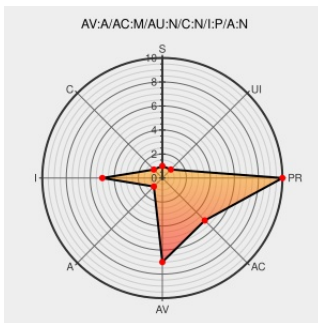
CVE-2013-0571

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Application Support Facility](#) from [Ibm](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in IBM Document Connect for Application Support Facility (aka DC4ASF) before 1.0.0.1218 in Application Support Facility (ASF) 3.4 for z/OS on Windows, Linux, and AIX allows remote attackers to inject arbitrary web script or HTML via a crafted URL.

CVE-2013-0571 has been assigned by psirt@us.ibm.com to track the vulnerability

CVSS2 Score: **2.9 - LOW**

Access
Vector

Access
Complexity

Authentication

ADJACENT_NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

IBM X-Force Exchange

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

[XF asf-cve20130571-xss\(83246\)](#)

Multiple vulnerabilities in feature Document Connect for ASF on LUW platforms

[Vendor Advisory](#)
www-01.ibm.com
text/html

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21635328](http://www-01.ibm.com/support/docview.wss?uid=swg21635328)

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 OIDs associated with this CVE

There are currently no CIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Application Support Facility	3.4.0	-	All	All
Application	Ibm	Application Support Facility	3.4.0	-	All	All
Application	Ibm	Application Support Facility	3.4.0	-	All	All
Application	Ibm	Application Support Facility	3.4.0	-	All	All
Application	Ibm	Application Support Facility	3.4.0	-	All	All
Application	Ibm	Application Support Facility	3.4.0	-	All	All
Application	Ibm	Application Support Facility	3.4.0	-	All	All
Application	Ibm	Application Support Facility	3.4.0	-	All	All
Application	Ibm	Application Support Facility	3.4.0	-	All	All
Application	Ibm	Document Connect For Application Support Facility	All	All	All	All

cpe:2.3:a:ibm:application_support_facility:3.4.0:-:*:*:aix:*:*:

cpe:2.3:a:ibm:application_support_facility:3.4.0:-:*:*:linux_kernel:*:*:

cpe:2.3:a:ibm:application_support_facility:3.4.0:-:*:*:windows:*:*:

cpe:2.3:a:ibm:application_support_facility:3.4.0:-:*:*:z/os:*:*:

cpe:2.3:a:ibm:application_support_facility:3.4.0:-:*:*:z/os:*:*:

cpe:2.3:a:ibm:application_support_facility:3.4.0:-:*:*:aix:*:*:

cpe:2.3:a:ibm:application_support_facility:3.4.0:-:*:*:linux_kernel:*:*:

cpe:2.3:a:ibm:application_support_facility:3.4.0:-:*:*:windows:*:*:

cpe:2.3:a:ibm:application_support_facility:3.4.0:-:*:*:z/os:*:*:

cpe:2.3:a:ibm:document_connect_for_application_support_facility:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

