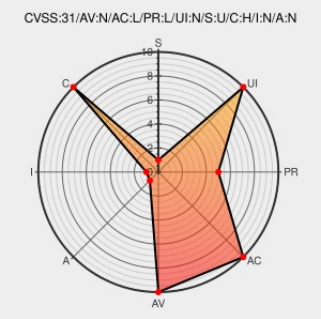
CVE-2015-5072

Published on: 01/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-5072

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



Certain versions of Remedy Ar System Server from Bmc contain the following vulnerability:

The BIRT Engine servlet in the AR System Mid Tier component before 9.0 SP1 for BMC Remedy AR System Server allows remote authenticated users to "navigate" to arbitrary local files via the __imageid parameter.

CVE-2015-5072 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Resolving BIRT Security Issues ISS04485990 (CVE... | BMC Communities	Vendor Advisory, communities.bmc.com, text/html	CONFIRM communities.bmc.com/docs/DOC-77816
BMC Remedy AR 8.1 / 9.0 File Inclusion ≈ Packet	Third Party Advisory	MISC packetstormsecurity.com/files/133689/BMC-

Storm	VDB Entry packetstormsecurity.com text/html	Remedy-AR-8.1-9.0-File-Inclusion.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bmc	Remedy Ar System Server	8.0	All	All	All
Application	Bmc	Remedy Ar System Server	9.0	All	All	All
Application	Bmc	Remedy Ar System Server	8.0	All	All	All
Application	Bmc	Remedy Ar System Server	9.0	All	All	All

cpe:2.3:a:bmc:remedy_ar_system_server:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:bmc:remedy_ar_system_server:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:bmc:remedy_ar_system_server:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:bmc:remedy_ar_system_server:9.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→