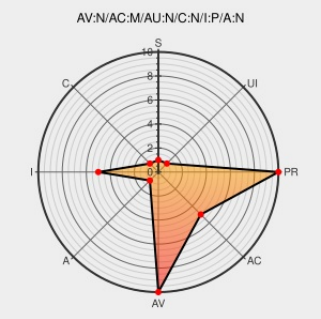
CVE-2012-2278

Published on: 07/13/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:26 PM UTC

CVE-2012-2278

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



Certain versions of Rsa Authentication Manager from Emc contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in the (1) Self-Service Console and (2) Security Console in EMC RSA Authentication Manager 7.1 before SP4 P14 and RSA SecurID Appliance 3.0 before SP4 P14 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVE-2012-2278 has been assigned by security_alert@emc.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	archives.neohapsis.com Inactive Link Not Archived	BUGTRAQ 20120711 ESA-2012-023: RSA Authentication Manager Multiple Vulnerabilities

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Rsa Authentication Manager	7.0	All	All	All
Application	Emc	Rsa Authentication Manager	7.1	All	All	All
Application	Emc	Rsa Authentication Manager	7.1	sp3	All	All
Application	Emc	Rsa Authentication Manager	7.0	All	All	All
Application	Emc	Rsa Authentication Manager	7.1	All	All	All
Application	Emc	Rsa Authentication Manager	7.1	sp3	All	All
Application	Emc	Rsa Authentication Manager	All	sp4	All	All
Application	Rsa	Authentication Manager	7.1	sp42	All	All
Application	Rsa	Authentication Manager	7.1	sp42	All	All
Application	Rsa	Securid Appliance	2.0	All	All	All
Application	Rsa	Securid Appliance	2.0.1	All	All	All
Application	Rsa	Securid Appliance	2.0.2	All	All	All
Application	Rsa	Securid Appliance	3.0	All	All	All
Application	Rsa	Securid Appliance	3.0	sp2	All	All
Application	Rsa	Securid Appliance	3.0	sp3	All	All
Application	Rsa	Securid Appliance	3.0	sp4	All	All
Application	Rsa	Securid Appliance	2.0	All	All	All
Application	Rsa	Securid Appliance	2.0.1	All	All	All
Application	Rsa	Securid Appliance	2.0.2	All	All	All
Application	Rsa	Securid Appliance	3.0	All	All	All
Application	Rsa	Securid Appliance	3.0	sp2	All	All
Application	Rsa	Securid Appliance	3.0	sp3	All	All
Application	Rsa	Securid Appliance	3.0	sp4	All	All

cpe:2.3:a:emc:rsa_authentication_manager:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:emc:rsa_authentication_manager:7.1:*:*:*:*:*:*:*:

cpe:2.3:a:emc:rsa_authentication_manager:7.1:sp3:*:*:*:*:*:*:

cpe:2.3:a:emc:rsa_authentication_manager:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:emc:rsa_authentication_manager:7.1:*:*:*:*:*:*:*:

cpe:2.3:a:emc:rsa_authentication_manager:7.1:sp3:*:*:*:*:*:*:

cpe:2.3:a:emc:rsa_authentication_manager:*:sp4:*:*:*:*:*:*:

cpe:2.3:a:rsa:authentication_manager:7.1:sp42:*:*:*:*:*:*:

cpe:2.3:a:rsa:authentication_manager:7.1:sp42:*:*:*:*:*:*:

cpe:2.3:a:rsa:authentication_manager:7.1:sp42:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:3.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:3.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:3.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:3.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:3.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:rsa:securid_appliance:3.0:sp4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→