



CVE-2015-6851

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-6851
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-23 03:59:00 UTC
Updated	2016-12-07 18:22:00 UTC
Description	EMC RSA SecurID Web Agent before 8.0 allows physically proximate attackers to bypass the privacy-screen protection me

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rsa	Securid Web Agent	All	All	All	All

References

Reference	Source	Link
Bugtraq: ESA-2015-177: RSA SecurID(r) Web Agent Authentication Bypass Vulnerability	BUGTRAQ	seclists.org
RSA SecurID Web Agent Re-Authentication Bug Lets Local Users Bypass Authentication - SecurityTracker	SECTRACK	www.securitytrac
RSA SecurID Web Agent CVE-2015-6851 Local Authentication Bypass Vulnerability	BID	www.securityfoc
RSA SecurID Web Agent Authentication Bypass ~ Packet Storm	MISC	packetstormsecu
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)