



CVE-2015-3163

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2015-3163
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-06 21:29:00 UTC
Updated	2020-03-09 18:39:00 UTC
Description	The admin pages for power types and key types in Beaker before 20.1 do not have any access controls, which allows remo

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Beaker	20.0	-	All	All
Application	Redhat	Beaker	20.0	rc1	All	All
Application	Redhat	Beaker	20.0	-	All	All
Application	Redhat	Beaker	20.0	rc1	All	All
Application	Redhat	Beaker	All	All	All	All

References

Reference	Source	Link	Tags
Beaker CVE-2015-3163 Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party A
1215034 – (CVE-2015-3163) anonymous users can modify key types and power types	CONFIRM	bugzilla.redhat.com	Exploit, Issue
404 Not Found	CONFIRM	beaker-project.org	Release Note
oss-security - beaker vulns fixed in version 20.1	MLIST	www.openwall.com	Mailing List, T
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)