



CVE-2014-3702

Published on: 10/16/2017 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:09 AM UTC

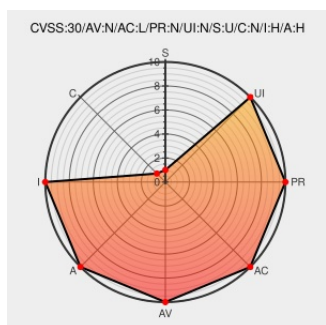
CVE-2014-3702

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Edeploy](#) from [Redhat](#) contain the following vulnerability:

Directory traversal vulnerability in eNovance eDeploy allows remote attackers to create arbitrary directories and files and consequently cause a denial of service (resource consumption) via a .. (dot dot) the session parameter.

CVE-2014-3702 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.4 - MEDIUM**

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

CVE References

Description	Tags	Link
1153470 – (CVE-2014-3702) CVE-2014-3702 eDeploy: Path traversal in the session parameter	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1153470

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Edeploy	0.1.0	All	All	All
Application	Redhat	Edeploy	0.2.0	All	All	All
Application	Redhat	Edeploy	1.4.0	All	All	All
Application	Redhat	Edeploy	1.5.0	All	All	All
Application	Redhat	Edeploy	h.1.0.0	All	All	All
Application	Redhat	Edeploy	h.1.1.0	All	All	All
Application	Redhat	Edeploy	h.1.2.0	All	All	All
Application	Redhat	Edeploy	h.1.3.0	All	All	All
Application	Redhat	Edeploy	0.1.0	All	All	All
Application	Redhat	Edeploy	0.2.0	All	All	All
Application	Redhat	Edeploy	1.4.0	All	All	All
Application	Redhat	Edeploy	1.5.0	All	All	All
Application	Redhat	Edeploy	h.1.0.0	All	All	All
Application	Redhat	Edeploy	h.1.1.0	All	All	All
Application	Redhat	Edeploy	h.1.2.0	All	All	All
Application	Redhat	Edeploy	h.1.3.0	All	All	All
cpe:2.3:a:redhat:edeploy:0.1.0:****:*:*:						
cpe:2.3:a:redhat:edeploy:0.2.0:****:*:*:						
cpe:2.3:a:redhat:edeploy:1.4.0:****:*:*:						
cpe:2.3:a:redhat:edeploy:1.5.0:****:*:*:						
cpe:2.3:a:redhat:edeploy:h.1.0.0:****:*:*:						
cpe:2.3:a:redhat:edeploy:h.1.1.0:****:*:*:						
cpe:2.3:a:redhat:edeploy:h.1.2.0:****:*:*:						
cpe:2.3:a:redhat:edeploy:h.1.3.0:****:*:*:						

cpe:2.3:a:redhat:edeploy:0.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:0.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.4.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.5.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.3.0:*:*:*:*:*:

cpe:2.3:a:redhat:edeploy:0.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:0.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.4.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.5.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.3.0:*:*:*:*:*:

cpe:2.3:a:redhat:edeploy:0.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:0.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.4.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.5.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.3.0:*:*:*:*:*:

cpe:2.3:a:redhat:edeploy:0.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:0.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.4.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.5.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.3.0:*:*:*:*:*:

cpe:2.3:a:redhat:edeploy:0.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:0.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.4.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.5.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.3.0:*:*:*:*:*:

cpe:2.3:a:redhat:edeploy:0.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:0.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.4.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.5.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.3.0:*:*:*:*:*:

cpe:2.3:a:redhat:edeploy:0.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:0.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.4.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.5.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.3.0:*:*:*:*:*:

cpe:2.3:a:redhat:edeploy:0.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:0.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.4.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:1.5.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.0.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.1.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.2.0:*:*:*:*:*:
cpe:2.3:a:redhat:edeploy:h.1.3.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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