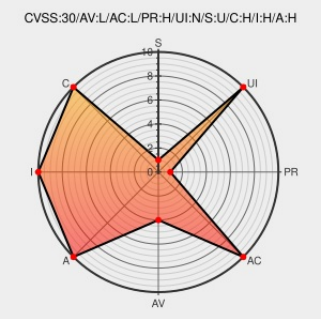
CVE-2017-15097

Published on: 07/27/2018 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:28:00 PM UTC

CVE-2017-15097

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



Certain versions of Enterprise Linux Desktop from Redhat contain the following vulnerability:

Privilege escalation flaws were found in the Red Hat initialization scripts of PostgreSQL. An attacker with access to the postgres user account could use these flaws to obtain root access on the server machine.

CVE-2017-15097 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Red Hat** - **postgresql init script** version **= all**

CVSS3 Score: 6.7 - MEDIUM

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2017:3403

1508985 – (CVE-2017-15097) CVE-2017-15097 postgresql: Start scripts permit database administrator to modify root-owned files	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-15097
Red Hat PostgreSQL Race Condition in Initialization Scripts Lets Local Users Obtain Root Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1039983
1508985 – (CVE-2017-15097) CVE-2017-15097 postgresql: Start scripts permit database administrator to modify root-owned files	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1508985
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2017:3402
CVE-2017-15097 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2017-15097
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2017:3404
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2017:3405

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating	Redhat	Enterprise Linux Server Eus	7.5	All	All	All

System						
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

- cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_server_eus:7.4:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_server_eus:7.4:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→