



# CVE-2018-1111

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

## Summary

<b>CVE</b>	CVE-2018-1111
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-05-17 16:29:00 UTC
<b>Updated</b>	2023-02-12 23:32:00 UTC
<b>Description</b>	DHCP packages in Red Hat Enterprise Linux 6 and 7, Fedora 28, and earlier are vulnerable to a command injection flaw in

## Risk And Classification

**Problem Types:** CWE-77

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	26	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	27	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	28	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	26	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	27	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	28	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Virtualization</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Virtualization</a>	4.2	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Virtualization</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Virtualization</a>	4.2	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Virtualization Host</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Virtualization Host</a>	4.0	All	All	All

## References

### Reference

[SECURITY] Fedora 28 Update: dhcp-4.3.6-20.fc28 - package-announce - Fedora Mailing-Lists

Red Hat Customer Portal

[SECURITY] Fedora 27 Update: dhcp-4.3.6-10.fc27 - package-announce - Fedora Mailing-Lists

Bug 1567974 – CVE-2018-1111 dhcp: Command injection vulnerability in the DHCP client NetworkManager integration script

Malformed Request

Red Hat Customer Portal
[SECURITY] Fedora 28 Update: dhcp-4.3.6-20.fc28 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 26 Update: dhcp-4.3.5-11.fc26 - package-announce - Fedora Mailing-Lists
[R1] TenableCore Web Application Scanner v20180702 Fixes Third-party Vulnerabilities - Security Advisory   Tenable®
DCIM Support
Red Hat Customer Portal
CVE-2018-1111 - Red Hat Customer Portal
DynoRoot DHCP Client - Command Injection
[SECURITY] Fedora 27 Update: dhcp-4.3.6-10.fc27 - package-announce - Fedora Mailing-Lists
DHCP Client Script Code Execution Vulnerability - CVE-2018-1111 - Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
1567974 – (CVE-2018-1111) CVE-2018-1111 dhcp: Command injection vulnerability in the DHCP client NetworkManager integration script
Red Hat Customer Portal
DHCP Client - Command Injection 'DynoRoot' (Metasploit)
Red Hat Customer Portal
Red Hat DHCP NetworkManager Script Component Lets Remote Users on the Local Network Execute Arbitrary Commands with Root Privileges
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
[SECURITY] Fedora 26 Update: dhcp-4.3.5-11.fc26 - package-announce - Fedora Mailing-Lists
CVE Program record
NVD vulnerability detail



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](#)**