



# CVE-2018-10897

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

## Summary

<b>CVE</b>	CVE-2018-10897
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-08-01 17:29:00 UTC
<b>Updated</b>	2023-02-13 04:51:00 UTC
<b>Description</b>	A directory traversal issue was found in reposync, a part of yum-utils, where reposync fails to sanitize paths in remote repos

## Risk And Classification

**Problem Types:** CWE-59

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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="#">Virtualization</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization</a>	4.0	All	All	All
Application	<a href="#">Rpm</a>	<a href="#">Yum-utils</a>	All	All	All	All
Application	<a href="#">Rpm-software-management Project</a>	<a href="#">Yum-utils</a>	All	All	All	All

## References

### Reference

reposync: check for .. in remote paths. BZ 1506205 by dmnks · Pull Request #43 · rpm-software-management/yum-utils · GitHub

CVE-2018-10897 - Red Hat Customer Portal

1600221 – (CVE-2018-10897) CVE-2018-10897 yum-utils: reposync: improper path validation may lead to directory traversal

Red Hat Enterprise Virtualization Path Validation Flaw in 'reposync' Lets Remote Users Modify Files on the Target System - SecurityTracker

DCIM Support

Red Hat Customer Portal

Red Hat Customer Portal

reposync: prevent path traversal. BZ 1552328 · rpm-software-management/yum-utils@6a8de06 · GitHub

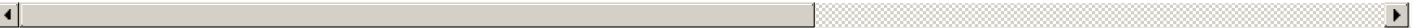
reposync: refactor: sanitize remote\_path usage · rpm-software-management/yum-utils@7554c01 · GitHub

Red Hat Customer Portal

1600221 – (CVE-2018-10897) CVE-2018-10897 yum-utils: reposync: improper path validation may lead to directory traversal

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](#)