



# CVE-2021-42374

Published on: 11/15/2021 12:00:00 AM UTC

Last Modified on: 03/31/2022 04:29:00 PM UTC

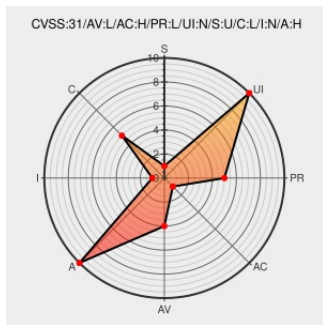
## CVE-2021-42374

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

An out-of-bounds heap read in Busybox's unlzma applet leads to information leak and denial of service when crafted LZMA-compressed input is decompressed. This can be triggered by any applet/format that

CVE-2021-42374 has been assigned by security@jfrog.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **busybox** - busybox version < 1.34.0

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>LOCAL</b>	<b>HIGH</b>	<b>LOW</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>LOW</b>	<b>NONE</b>	<b>HIGH</b>

CVSS2 Score: **3.3 - LOW**

Access Vector	Access Complexity	Authentication
<b>LOCAL</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>PARTIAL</b>	<b>NONE</b>	<b>PARTIAL</b>

## CVE References

Description	Tags	Link
November 2021 BusyBox Vulnerabilities in NetApp Products   NetApp Product Security	<a href="#">security.netapp.com</a> <a href="#">text/html</a>	<b>CONFIRM</b> <a href="https://security.netapp.com/advisory/ntap-20211223-0002/">security.netapp.com/advisory/ntap-20211223-0002/</a>

Unboxing BusyBox - 14 new vulnerabilities uncovered by Claroty and JFrog | JFrog

[jfrog.com](#)  
[text/html](#)

 MISC [jfrog.com/blog/unboxing-busybox-14-new-vulnerabilities-uncovered-by-claroty-and-jfrog/](https://jfrog.com/blog/unboxing-busybox-14-new-vulnerabilities-uncovered-by-claroty-and-jfrog/)

[SECURITY] Fedora 33 Update: busybox-1.34.1-1.fc33 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](https://lists.fedoraproject.org)  
[text/html](#)

 FEDORA [FEDORA-2021-5a95823596](#)

No Description Provided

[lists.fedoraproject.org](https://lists.fedoraproject.org)

 FEDORA [FEDORA-2021-c52c0fe490](#)

Inactive Link Not Archived















By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

## Related QID Numbers

- [198599](#) Ubuntu Security Notification for BusyBox Vulnerabilities (USN-5179-1)
- [282073](#) Fedora Security Update for busybox (FEDORA-2021-c52c0fe490)
- [282074](#) Fedora Security Update for busybox (FEDORA-2021-5a95823596)
- [376047](#) BusyBox Information Leak and Denial of Service (DoS) Vulnerability
- [500082](#) Alpine Linux Security Update for busybox
- [501387](#) Alpine Linux Security Update for busybox
- [501733](#) Alpine Linux Security Update for busybox
- [501950](#) Alpine Linux Security Update for busybox
- [671290](#) EulerOS Security Update for busybox (EulerOS-SA-2022-1250)
- [671329](#) EulerOS Security Update for busybox (EulerOS-SA-2022-1238)
- [671364](#) EulerOS Security Update for busybox (EulerOS-SA-2022-1303)
- [671377](#) EulerOS Security Update for busybox (EulerOS-SA-2022-1287)
- [730371](#) McAfee Web Gateway Multiple Vulnerabilities (WP-3335,WP-4131,WP-4159,WP-4237,WP-4259,WP-4329,WP-4348,WP-4355,WP-4376,WP-4407,WP-4421)
- [751624](#) SUSE Enterprise Linux Security Update for busybox (SUSE-SU-2022:0135-1)
- [751633](#) OpenSUSE Security Update for busybox (openSUSE-SU-2022:0135-1)
- [752794](#) SUSE Enterprise Linux Security Update for busybox (SUSE-SU-2022:3959-1)
- [752903](#) SUSE Enterprise Linux Security Update for busybox (SUSE-SU-2022:4253-1)
- [900457](#) Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6185)
- [900884](#) Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6343-1)

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Busybox</a>	<a href="#">Busybox</a>	ΔII	ΔII	ΔII	ΔII

Application	busybox	busybox	All	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	All	All
Hardware  	<a href="#">Netapp</a>	<a href="#">H300e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300e Firmware</a>	-	All	All	All
Hardware  	<a href="#">Netapp</a>	<a href="#">H300s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300s Firmware</a>	-	All	All	All
Hardware  	<a href="#">Netapp</a>	<a href="#">H410s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410s Firmware</a>	-	All	All	All
Hardware  	<a href="#">Netapp</a>	<a href="#">H500e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500e Firmware</a>	-	All	All	All
Hardware  	<a href="#">Netapp</a>	<a href="#">H500s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500s Firmware</a>	-	All	All	All
Hardware  	<a href="#">Netapp</a>	<a href="#">H700e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700e Firmware</a>	-	All	All	All
Hardware  	<a href="#">Netapp</a>	<a href="#">H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700s Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All


  

<code>cpe:2.3:a:busybox:busybox:.*:.*:.*:.*:.*:.*:.*</code>
<code>cpe:2.3:o:fedoraproject:fedora:33:.*:.*:.*:.*:.*:.*</code>
<code>cpe:2.3:o:fedoraproject:fedora:34:.*:.*:.*:.*:.*:.*</code>
<code>cpe:2.3:a:netapp:cloud_backup:-:.*:.*:.*:.*:.*:.*</code>
<code>cpe:2.3:h:netapp:h300e:-:.*:.*:.*:.*:.*:.*</code>
<code>cpe:2.3:o:netapp:h300e_firmware:-:.*:.*:.*:.*:.*:.*</code>
<code>cpe:2.3:h:netapp:h300s:-:.*:.*:.*:.*:.*:.*</code>
<code>cpe:2.3:o:netapp:h300s_firmware:-:.*:.*:.*:.*:.*:.*</code>



cpe:2.3:h:netapp:h410s:-:*:*:*:*:*:*:
cpe:2.3:o:netapp:h410s_firmware:-:*:*:*:*:*:*:
cpe:2.3:h:netapp:h500e:-:*:*:*:*:*:*:
cpe:2.3:o:netapp:h500e_firmware:-:*:*:*:*:*:*:
cpe:2.3:h:netapp:h500s:-:*:*:*:*:*:*:
cpe:2.3:o:netapp:h500s_firmware:-:*:*:*:*:*:*:
cpe:2.3:h:netapp:h700e:-:*:*:*:*:*:*:
cpe:2.3:o:netapp:h700e_firmware:-:*:*:*:*:*:*:
cpe:2.3:h:netapp:h700s:-:*:*:*:*:*:*:
cpe:2.3:o:netapp:h700s_firmware:-:*:*:*:*:*:*:
cpe:2.3:a:netapp:hci_management_node:-:*:*:*:*:*:*:
cpe:2.3:a:netapp:solidfire:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-42374 : An out-of-bounds heap read in Busybox's unlzma applet leads to information leak and denial of serv... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-11-15 21:11:16

[← 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](https://status.cve.report)**