

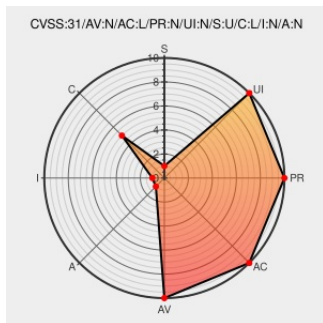


CVE-2019-19800

Published on: 02/06/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-19800

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Manageengine Applications Manager](#) from [Zohocorp](#) contain the following vulnerability:

Zoho ManageEngine Applications Manager 14 before 14520 allows a remote unauthenticated attacker to disclose OS file names via FailOverHelperServlet.

CVE-2019-19800 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
ManageEngine - IT Operations and Service Management Software	Product www.manageengine.com text/html	MISC www.manageengine.com
eLeN3Re / CVE-2019-19800 · GitLab	Third Party Advisory	MISC gitlab.com/eLeN3Re/CVE-2019-19800/

gitlab.com
text/html

No Description Provided

[Release Notes](#)
www.manageengine.com
[text/html](#)

 MISC
www.manageengine.com/products/applications_manager/release-notes.html

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zohocorp	Manageengine Applications Manager	14.0	-	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14000	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14010	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14020	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14030	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14040	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14050	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14060	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14070	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14071	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14072	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14073	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14080	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14090	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14100	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14110	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14120	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14130	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14140	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14150	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14160	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14170	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14180	All	All
Application	Zohocorp	Manageengine Applications Manager	14.0	build14190	All	All

[illegible]

[illegible]

[illegible]

[illegible]

cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14290:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14300:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14310:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14330:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14331:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14332:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14340:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14350:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14360:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14361:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14370:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14380:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14390:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14400:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14401:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14410:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14420:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14430:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14440:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14450:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14460:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14470:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14480:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14490:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14500:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14510:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:-:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14000:*****:
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14010:*****:

```
cpe:2.3:a:zonocorp:manageengine_applications_manager:14.0:build 14010:":":":":":
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14020:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14030:*.:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14040:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14050:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14060:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14070:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14071:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14072:*.*.*.*.:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14073:*:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14080:*.***.***:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14090:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14100:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14110:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14120:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14130:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14140:*.*.*.*.*.:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14150:*.***.***:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14160:*.***.*.*.*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14170:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14180:*.*.*.*.*.:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14190:*.*.*.*.*.:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14200:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14210:*.***.*.*.*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14220:*.***.*.*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14230:*.***.*.*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14240:*.***.*.*.*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14250:*.***.*.*.*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14260:*.***.*.*.*
```



```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14261:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14262:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14270:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14280:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14290:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14300:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14310:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14330:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14331:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14332:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14340:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14350:*:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14360:*.*.*.*.:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14361:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14370:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14380:*:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14390:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14400:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14401:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14410:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14420:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14430:*.***.***:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14440:*:*:*:*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14450:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14460:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14470:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14480::*:.*:*
```

```
cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14490:*:*:*:*:*
```

cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14500:*****:

cpe:2.3:a:zohocorp:manageengine_applications_manager:14.0:build14510:*****:

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](#)