



ManageEngine administrator visualizes the page: <Server > Software" the administrator of ManageEngine can control what software is installed on the workstation. This table shows all the installed program names in the Software column. In this field, a remote attacker can inject malicious code in order to execute it when the ManageEngine administrator visualizes this page." />

CVE-2019-15083

Published on: 05/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

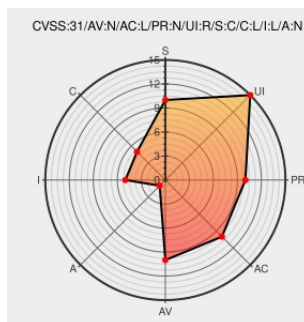
CVE-2019-15083

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

Default installations of Zoho ManageEngine ServiceDesk Plus 10.0 before 10500 are vulnerable to XSS injected by a workstation local administrator. Using the installed program names of the computer as a vector, the local administrator can execute code on the Manage Engine ServiceDesk administrator side. At "Asset Home > Server >

<workstation> > software" the administrator of ManageEngine can control what software is installed on the workstation. This table shows all the installed program names in the Software column. In this field, a remote attacker can inject malicious code in order to execute it when the ManageEngine administrator visualizes this page.

CVE-2019-15083 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

PARTIAL

NONE

CVE References

Description	Tags	Link
ManageEngine ServiceDesk Plus - README	Release Notes Vendor Advisory www.manageengine.com text/html	 MISC www.manageengine.com/products/service-desk/readme.html
ManageEngine Service Desk 10.0 Cross Site Scripting ≈ Packet Storm	Third Party Advisory packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/157717/ManageEngine-Service-Desk-10.0-Cross-Site-Scripting.html
ManageEngine Service Desk 10.0 - Cross-Site Scripting - Java webapps Exploit	Third Party Advisory www.exploit-db.com Proof of Concept text/html	 MISC www.exploit-db.com/exploits/48473
No Description Provided	Release Notes Vendor Advisory www.manageengine.com text/html	 MISC www.manageengine.com/products/service-desk/on-premises/readme.html#readme105

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 Servicedesk Plus	10.0.0	-	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10000	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10001	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10002	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10003	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10004	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10005	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10006	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10007	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10008	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10009	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10010	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10011	All	All
Application	Zohocorp	Manageengine Servicedesk Plus	10.0.0	10012	All	All


```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10001:::~
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10002:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10003:*:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10004:*:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10005:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10006:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10007:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10008:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10009:*.***.***:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10010::*:.*:.*
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10011:*.*.*.*.:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10012:*.***.***.***
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10013:*.***.***.***
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10014:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10015::*:.*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10016:*.***.***:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10017:*.***.***:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10018:*.***.***:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10019::*:.*:.*
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10020:::*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10021:::*.*.*.*.*
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:-:*:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10000:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10001:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10002:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10003:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10004:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10005:*:*:*:*:
```

```
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10006:*:*:*:*:
```

cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10007:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10008:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10009:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10010:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10011:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10012:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10013:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10014:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10015:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10016:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10017:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10018:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10019:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10020:*****:
cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:10.0.0:10021:*****:

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](#)