



CVE-2018-14366

Published on: 09/06/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:43 PM UTC

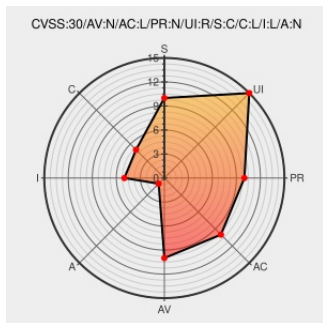
CVE-2018-14366

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Pulse Connect Secure](#) from [Pulsesecure](#) contain the following vulnerability:

download.cgi in Pulse Secure Pulse Connect Secure 8.1RX before 8.1R13 and 8.3RX before 8.3R4 and Pulse Policy Secure through 5.2RX before 5.2R10 and 5.4RX before 5.4R4 have an Open Redirect Vulnerability.

CVE-2018-14366 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: **5.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Public KB - SA43877 - 2018-08 Security Bulletin: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure / Pulse Secure Desktop 9.0R1/9.0R2	Vendor Advisory kb.pulsesecure.net text/html	CONFIRM kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA43877

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	Pulsesecure	Pulse Connect Secure	8.1	All	All	All
Application	Pulsesecure	Pulse Connect Secure	8.1r1.0	All	All	All
Application	Pulsesecure	Pulse Connect Secure	8.1rx	All	All	All
Application	Pulsesecure	Pulse Connect Secure	8.3	All	All	All
Application	Pulsesecure	Pulse Connect Secure	8.3rx	All	All	All
Application	Pulsesecure	Pulse Connect Secure	8.1	All	All	All
Application	Pulsesecure	Pulse Connect Secure	8.1r1.0	All	All	All
Application	Pulsesecure	Pulse Connect Secure	8.1rx	All	All	All
Application	Pulsesecure	Pulse Connect Secure	8.3	All	All	All
Application	Pulsesecure	Pulse Connect Secure	8.3rx	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r1.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r2.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r3.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r3.2	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r4.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r5.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r6.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r7.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r7.1	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r8.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r9.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r9.1	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2rx	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.4r1	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.4r2	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.4r2.1	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.4r3	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.4rx	All	All	All

Application	Pulsesecure	Pulse Policy Secure	5.2r1.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r2.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r3.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r3.2	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r4.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r5.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r6.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r7.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r7.1	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r8.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r9.0	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2r9.1	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.2rx	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.4r1	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.4r2	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.4r2.1	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.4r3	All	All	All
Application	Pulsesecure	Pulse Policy Secure	5.4rx	All	All	All
cpe:2.3:a:pulsesecure:pulse_connect_secure:8.1:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_connect_secure:8.1r1.0:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_connect_secure:8.1rx:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_connect_secure:8.3:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_connect_secure:8.3rx:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_connect_secure:8.1:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_connect_secure:8.1r1.0:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_connect_secure:8.1rx:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_connect_secure:8.3:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_connect_secure:8.3rx:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r1.0:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r2.0:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r3.0:*****:.*:						
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r3.2:*****:.*:						

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r4.0:*.:*:*:*:*.*
```

cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r5.0:*.:*:*:*:*:

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r6.0:*.:*:*:*:*.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r7.0:*.***.***.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r7.1:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r8.0:*:*:*:*:*:
```

cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r9.0:*.:*:*:*:*:

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r9.1:*.:*:*:*:*.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2rx:*.:*:*:*:*.*
```

cpe:2.3:a:pulsesecure:pulse_policy_secure:5.4r1:.*:.*:.*:.*:.*:.*:.*

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.4r2:*.:*:*:*:*.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.4r2.1:*.***.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.4r3:*.:*:*:*:*.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.4rx:*:*:*:*:*:
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r1.0:*.:*:*:*:*.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r2.0:*.:*:*:*:*.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r3.0:*.:.:.:.:.:
```

```
cpe:2.3:a:pulsesecure:pulse policy secure:5.2r3.2:*.***.***.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r4.0:*.***.***.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r5.0:*.***.***.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r6.0:*.:*:*:*:*.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r7.0:*.:.:.:.:.:
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r7.1:*.***.***.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r8.0:::*.*.*.*.*.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r9.0:*.:*:*:*:*.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2r9.1:*.***.***.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.2rx:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.4r1:::*:*:*.*.*
```

cpe:2.3:a:pulsesecure:pulse_policy_secure:5.4r2:*:*:*:*:*:	
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.4r2.1:*:*:*:*:*:	
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.4r3:*:*:*:*:*:	
cpe:2.3:a:pulsesecure:pulse_policy_secure:5.4rx:*:*:*:*:*:	
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](#)