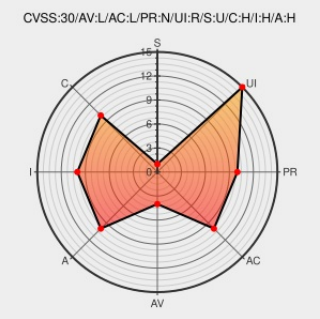
CVE-2018-6514

Published on: 06/11/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:47 PM UTC

CVE-2018-6514

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows from Microsoft contain the following vulnerability:

In Puppet Agent 1.10.x prior to 1.10.13, Puppet Agent 5.3.x prior to 5.3.7, Puppet Agent 5.5.x prior to 5.5.2, Facter on Windows is vulnerable to a DLL preloading attack, which could lead to a privilege escalation.

CVE-2018-6514 has been assigned by security@puppet.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Puppet** - **Puppet Agent** version **Puppet Agent 1.10.x prior to 1.10.13, Puppet Agent 5.3.x prior to 5.3.7, Puppet Agent 5.5.x prior to 5.5.2**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2018-6514 - Facter Tries to Load DLLs from the Current Working Directory | Puppet.com	Vendor Advisory puppet.com	CONFIRM puppet.com/security/cve/CVE-2018-6514

text/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
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Puppet	Puppet	All	All	All	All
Application	Puppet	Puppet	All	All	All	All

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:a:puppet:puppet:*:*:*:*:*:*:*:*:

cpe:2.3:a:puppet:puppet:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→