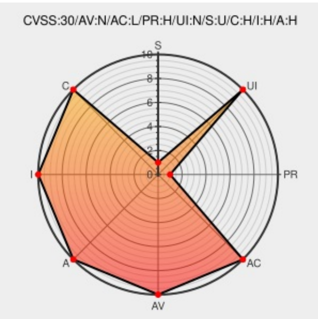
CVE-2018-7567

Published on: 03/04/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:38 PM UTC

CVE-2018-7567

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



Certain versions of Otrs from Otrs contain the following vulnerability:

** DISPUTED ** In the Admin Package Manager in Open Ticket Request System (OTRS) 5.0.0 through 5.0.24 and 6.0.0 through 6.0.1, authenticated admins are able to exploit a Blind Remote Code Execution vulnerability by loading a crafted opm file with an embedded CodeInstall element to execute a command on the server during package installation. NOTE: the vendor disputes this issue stating "the behaviour is as designed and needed for different packages to be installed", "there is a security warning if the package is not verified by OTRS Group", and "there is the possibility and responsibility of an admin to check packages before installation which is possible as they are not binary."

CVE-2018-7567 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Access denied | 0day.today used Cloudflare to restrict access	Exploit Third Party Advisory 0day.today text/html Inactive Link Not Archived	MISC 0day.today/exploit/29938

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	Otrs	Otrs	6.0.0	All	All	All
Application	Otrs	Otrs	6.0.1	All	All	All
Application	Otrs	Otrs	6.0.0	All	All	All
Application	Otrs	Otrs	6.0.1	All	All	All
Application	Otrs	Otrs	All	All	All	All

cpe:2.3:a:otrs:otrs:6.0.0:*:*:*:*:*:*:

cpe:2.3:a:otrs:otrs:6.0.1:*:*:*:*:*:*:

cpe:2.3:a:otrs:otrs:6.0.0:*:*:*:*:*:*:

cpe:2.3:a:otrs:otrs:6.0.1:*:*:*:*:*:*:

cpe:2.3:a:otrs:otrs:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→