



CVE-2017-7357

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-7357
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-14 18:59:00 UTC
Updated	2018-10-09 20:01:00 UTC
Description	Hipchat Server before 2.2.3 allows remote authenticated users with Server Administrator level privileges to execute arbitrar

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Hipchat Server	All	All	All	All

References

Reference	Source	Link
HipChat Server Security Advisory 2017-04-12 - Atlassian Documentation	CONFIRM	confluence.atlassian.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
Atlassian Hipchat Server CVE-2017-7357 Remote Code Execution Vulnerability	BID	www.securityfocus.com
[HCPUB-2903] Potential RCE in Imports - Create and track feature requests for Atlassian products.	CONFIRM	jira.atlassian.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)