



CVE-2013-6366

Published on: 11/04/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:38 PM UTC

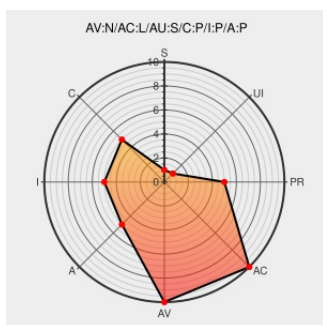
CVE-2013-6366

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Hyperic Hq](#) from [Vmware](#) contain the following vulnerability:

The Groovy script console in VMware Hyperic HQ 4.6.6 allows remote authenticated administrators to execute arbitrary code via a `Runtime.getRuntime().exec` call.

CVE-2013-6366 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.5 - MEDIUM**

**Access
Vector**

NETWORK

**Access
Complexity**

LOW

Authentication

SINGLE

**Confidentiality
Impact**

PARTIAL

**Integrity
Impact**

PARTIAL

**Availability
Impact**

PARTIAL

CVE References

Description

Tags

Link

VMware Hyperic HQ Groovy Script-Console Java Execution

[Exploit](#)

www.exploit-db.com

[Proof of Concept](#)

[text/x-ruby](#)

[EXPLOIT-DB 28962](#)

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)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Hyperic Hq	4.6.6	All	All	All
Application	Vmware	Hyperic Hq	4.6.6	All	All	All
cpe:2.3:a:vmware:hyperic_hq:4.6.6:*****::						
cpe:2.3:a:vmware:hyperic_hq:4.6.6:*****::						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID →		