



Low

CVSS

Availability

None

CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:S/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Theforeman	Foreman	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References	
Reference	Source
Fixes #16022 - Prevent stored XSS in host interface form by tbrisker · Pull Request #3714 · theforeman/foreman · GitHub	af854a3a-2127-4...
Bug #16022: CVE-2016-6320 - Network interface device identifiers may contain stored XSS on host form - Foreman	af854a3a-2127-4...
Foreman :: Security	af854a3a-2127-4...
Red Hat Satellite CVE-2016-6320 HTML Injection Vulnerability	af854a3a-2127-4...
Red Hat Customer Portal	af854a3a-2127-4...
Bug 1365785 – CVE-2016-6320 satellite6: stored XSS while provisioning new host	af854a3a-2127-4...
CVE-2016-6320 - Red Hat Customer Portal	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)