Bug 2437036 (CVE-2026-1961) - CVE-2026-1961 forman: Foreman: Remote Code Execution via command injection in WebSocket proxy

Keywords: Security

Status: NEW

Alias: CVE-2026-1961

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-02-05 10:42 UTC by OSIDB Bzimport

Modified: 2026-03-26 20:26 UTC (History)

CC List: 12 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2026:5970	0	None	None	None	2026-03-26 20:25:59 UTC
Red Hat Product Errata	RHSA-2026:5971	0	None	None	None	2026-03-26 20:26:55 UTC

OSIDB Bzimport 2026-02-05 10:42:27 UTC Description

Summary: A critical command injection vulnerability exists in Foreman's WebSocket proxy implementation (lib/ws_proxy.rb). The vulnerability occurs when constructing shell commands using unsanitized hostname values from compute resource providers. An attacker operating a malicious compute resource server (VMware vSphere, Libvirt, etc.) can achieve remote code execution on the Foreman server when an administrator accesses VM console functionality.

Requirements to exploit: An attacker needs to operate a malicious compute resource server (such as a fake vSphere server) that returns poisoned hostname values. The Foreman administrator must then configure this malicious server as a compute resource and attempt to access the VM console through the normal workflow.

Component affected: foreman

Version affected: Foreman <= 3.17.0 (confirmed), likely all versions from the past 4+ years (ws_proxy.rb unchanged since 2020)

Patch available: Yes (need to be reviewed and verified)

```
#
Line 44 - Sanitize host parameter
safe_host
= Shellwords.escape(host)
#
Use array form to prevent shell injection
cmd_array
= [
  'websockify',
  '--daemon',

"--idle-timeout=#{idle_timeout}",

"--timeout=#{timeout}",
  port.to_s,

"#{safe_host}:#{host_port}"
]
#
Add SSL options
cmd_array
+= ['--ssl-target'] if ssl_target
if
Setting[:websockets_encrypt]
  cmd_array
+= ['--cert', Setting[:websockets_ssl_cert]] if
Setting[:websockets_ssl_cert]
  cmd_array
+= ['--key', Setting[:websockets_ssl_key]] if
Setting[:websockets_ssl_key]
end
#
Execute without shell interpretation
Open3.popen3(*cmd_array)
do |stdin, stdout, stderr|
  #
```

```
... existing error handling
End
Version fixed (if any already): N/A


CVSS: Proposed by reporter -
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (Base Score: 8.8
High)


My understanding of the situation (6.8 Medium/High; Still
serious, but not "internet critical" –
CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H)
Impact (optional): This vulnerability allows remote code
execution as the foreman user, providing direct access to
Foreman's database credentials and encryption keys. This
enables decryption of all stored infrastructure credentials
(vCenter, AWS, SSH keys, API tokens), allowing the attacker to
pivot and compromise the entire managed infrastructure. Based
on Red Hat's classification, this would be considered Critical
impact due to the potential for complete infrastructure
compromise.
Embargo needed: Yes
Reason: Given it is command injection
Public date: Need to set default 90-days. There is no date
received from the reporter.


Acknowledgement: Houssam Sahli


Steps to reproduce if available:
1. Start malicious vSphere server (attacker system):
python3 malicious_vsphere_server.py
2. Configure Foreman compute resource (Foreman UI):
   - Navigate to: Infrastructure → Compute Resources → Create
Compute Resource
   - Provider: VMware
   - VCenter/Server: <attacker_ip> (malicious server address)
   - Username: user
   - Password: pass
   - Load Datacenters (it will load EvilDatacenter)
   - Display Type: VNC
   - Uncheck "VNC Console Passwords" and "Enable Caching"
   - Click "Submit"
3. Trigger exploitation:
   - Navigate to Virtual Machines tab
   - Locate "TestVM" in the list
   - Click Actions → Console
4. Verify RCE (Foreman server):
find /tmp -name "vsphere_rce.txt" 2>/dev/null
cat /tmp/systemd-private-*/tmp/vsphere_rce.txt
Expected output: foreman
```

errata-xmlrpc 2026-03-26 20:25:57 UTC Comment 2

```
This issue has been addressed in the following products:

  Red Hat Satellite 6.17 for RHEL 9
```

Via RHSA-2026:5970 https://access.redhat.com/errata/RHSA-2026:5970

errata-xmlrpc 2026-03-26 20:26:52 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat Satellite 6.16 for RHEL 8
  Red Hat Satellite 6.16 for RHEL 9

Via RHSA-2026:5971 https://access.redhat.com/errata/RHSA-2026:5971

Note

You need to log in before you can comment on or make changes to this bug.