Bug 1939701 (CVE-2021-20290) - CVE-2021-20290 smart_proxy_openscap: Clients can perform reserved actions on Foreman Server through OpenSCAP plugin for smart-proxy

Keywords: Security ×

Status: NEW

Alias: CVE-2021-20290

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 1939709

Blocks: 1937277 1945042

TreeView+ depends on / blocked

Reported: 2021-03-16 20:50 UTC by Yadnyawalk Tale

Modified: 2022-07-18 09:51 UTC (History)

CC List: 13 users (show)

Fixed In Version: smart_proxy_openscap 0.9.1

Doc Type: If docs needed, set a value

Doc Text: An improper authorization handling flaw was found in Foreman. The OpenSCAP plugin for the smart-proxy allows foreman clients to execute actions that should be limited to the Foreman Server. This flaw allows an authenticated local attacker to access and delete limited resources and also causes a denial of service on the Foreman server. The highest threat from this vulnerability is to integrity and system availability.

Clone Of:

Environment:

Last Closed:

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Yadnyawalk Tale 2021-03-16 20:50:13 UTC — Description

On Foreman, OpenSCAP plugin for smart-proxy introduce a flaw which allows any client to perform actions of Foreman Server. OpenSCAP plugin and a Client system that has Puppet installed with certs signed by Puppet CA or a Foreman with a client system that has a consumer certificate from the Katello CA; attacker can use this Client's certs to access the OpenSCAP API and perform actions which are only reserved for a Foreman server.

Yadnyawalk Tale 2021-03-16 20:50:21 UTC — Comment 1

Acknowledgments:

Name: Evgeni Golov (Red Hat)
Upstream: Foreman project

Yadnyawalk Tale 2021-03-16 20:50:24 UTC — Comment 2

Mitigation:

To mitigate the flaw, disable smart_proxy_openscap plugin from the Server. You can do that either by editing `/etc/foreman-proxy/settings.d/openscap.yml` and restarting `systemctl restart foreman-proxy.service`, or by running `foreman-installer --no-enable-foreman-proxy-plugin-openscap` command.

Yadnyawalk Tale 2021-03-18 19:36:15 UTC — Comment 6

Statement:

Red Hat Satellite 6 ship smart_proxy_openscap plugin which is affected by the flaw. The highest threat from this vulnerability is to integrity and system availability.

Lukas Zapletal 2021-04-06 14:32:52 UTC — Comment 7

Upstream patch: https://github.com/theforeman/smart_proxy_openscap/pull/80

(Pending review)

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