Bug 1891016 (CVE-2020-25715) - CVE-2020-25715 pki-core: XSS in the certificate search results

Keywords: Security ×

Status: CLOSED ERRATA
Alias: CVE-2020-25715
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: 1426572 1898055 1903211 ~~1934442~~ 1934278 1934676 1934678 1940561 1945155 1945156 1945157
Blocks: 1891015
TreeView+ depends on / blocked

Reported: 2020-10-23 14:42 UTC by Cedric Buissart
Modified: 2021-04-20 09:49 UTC (History)
CC List: 13 users (show)
Fixed In Version: pki-core 10.9.0
Doc Type: If docs needed, set a value
Doc Text: A flaw was found in pki-core. A specially crafted POST request can be used to reflect a DOM-based cross-site scripting (XSS) attack to inject code into the search query form which can get automatically executed. The highest threat from this vulnerability is to data integrity.
Clone Of:
Environment:
Last Closed: 2021-03-15 17:25:48 UTC

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

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2021:0819	0	None	None	None	2021-03-15 13:26:11 UTC
Red Hat Product Errata	RHSA-2021:0851	0	None	None	None	2021-03-16 13:48:19 UTC
Red Hat Product Errata	RHSA-2021:0975	0	None	None	None	2021-03-23 16:46:58 UTC

Cedric Buissart 2020-10-23 14:42:25 UTC — Description

The search query is reflected back to the user, and injected in a form, so that the user can click on the "next page", etc. However, a specially crafted POST request can be used to reflect a DOM XSS, which can get automatically executed.

The XSS requires the victim to have installed their RHCS certificate in the web browser. If that certificate has sufficient permissions, the XSS can be used to execute arbitrary code, including sending and signing arbitrary certificates.

Vulnerable page : /ca/ee/ca/listCerts (there might be other pages vulnerable to a similar attack)

```
document.write(
"<button NAME=begin onClick='doNext(this)' VALUE='|<<' width='72'>|<<</button>\n"+
"<button "+disabledUp+" NAME=up onClick='doNext(this)' VALUE='<' width='72'><</button>\n"+
[...]
"<INPUT TYPE=hidden NAME=skipNonValid VALUE='"+
(result.header.skipNonValid ? result.header.skipNonValid : "") + "'>\n"+
```

Several POST parameters, including `skipNonValid`, are being reflected back to the browser without having been sanitized by the server. An attacker can use that to inject JavaScript in the DOM.

Attack scenario :
A victim authenticated in RHCS web UI (the corresponding web browser has the required key/cert installed for client authentication), is tricked into clicking a button on an attacker-controlled website. The XSS can then be used to execute arbitrary JavaScript in the context of RHCS.

~~Eric Christensen~~ 2021-02-11 18:30:25 UTC — Comment 7

Mitigation:

Because the cross-site scripting (XSS) attack requires the victim to have their RHCS certificate installed in their web browser to be successful, it is recommended that web browser not hold the keys and that the user use the command line interface (CLI) instead.

Cedric Buissart 2021-03-02 15:27:57 UTC — Comment 8

Created pki-core tracking bugs for this issue:

Affects: fedora-all [~~bug 1931110~~]

Cedric Buissart 2021-03-03 20:44:42 UTC — Comment 11

Upstream fix :
https://github.com/dogtagpki/pki/commit/13f4c7fe7d71d42b46b25f3e8472ef7f35da5dd6

errata-xmlrpc 2021-03-15 13:26:11 UTC — Comment 16

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7.6 Extended Update Support

Via RHSA-2021:0819 https://access.redhat.com/errata/RHSA-2021:0819

Product Security DevOps Team 2021-03-15 17:25:48 UTC Comment 17

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2020-25715

errata-xmlrpc 2021-03-16 13:48:19 UTC Comment 18

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2021:0851 https://access.redhat.com/errata/RHSA-2021:0851

Cedric Buissart 2021-03-18 15:44:15 UTC Comment 19

Statement:

Red Hat Enterprise Linux 8.3 (pki-core 10.9.4) contains mitigations that prevents the vulnerability to be exploited. Red Hat Enterprise Linux version 8 prior to 8.3 are vulnerable to this version

errata-xmlrpc 2021-03-23 16:46:59 UTC Comment 20

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7.7 Extended Update Support

Via RHSA-2021:0975 https://access.redhat.com/errata/RHSA-2021:0975

errata-xmlrpc 2021-04-20 09:49:28 UTC Comment 21

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.2 Extended Update Support

Via RHSA-2021:1263 https://access.redhat.com/errata/RHSA-2021:1263