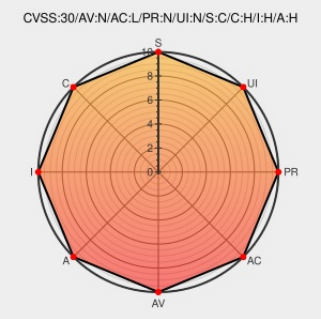
CVE-2015-7541

Published on: 01/08/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:11 PM UTC

CVE-2015-7541

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Colorscore from Colorscore Project contain the following vulnerability:

The initialize method in the Histogram class in lib/colorscore/histogram.rb in the colorscore gem before 0.0.5 for Ruby allows context-dependent attackers to execute arbitrary code via shell metacharacters in the (1) image_path, (2) colors, or (3) depth variable.

CVE-2015-7541 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 10 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
oss-security - Remote Command Injection in Ruby Gem colorscore <=0.0.4	www.openwall.com text/html	MLIST [oss-security] 20160104 Remote Command Injection in Ruby Gem col <=0.0.4
CVE-2015-7541: colorscore	web.archive.org	MISC rubysec.com/advisories/CVE-2015-7541/

Gem for Ruby lib/colorscore/histogram.rb Arbitrary Command Injection - RubySec	text/html Inactive Link Not Archived	
Fix CVE-2015-7541 · quadule/colorscore@570b5e8 · GitHub	Patch github.com text/html	CONFIRM github.com/quadule/colorscore/commit/570b5e854cecddd44d2047c44126aed95

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)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Colorscore Project	Colorscore	All	All	All	All

cpe:2.3:a:colorscore_project:colorscore:*:*:*:*:*:ruby:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→