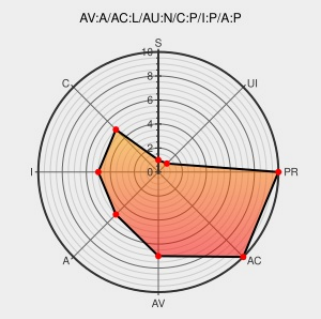
CVE-2013-6492

Published on: 02/14/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:25 AM UTC

CVE-2013-6492

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



Certain versions of Piranha from Ryan Ohara contain the following vulnerability:

The Piranha Configuration Tool in Piranha 0.8.6 does not properly restrict access to webpages, which allows remote attackers to bypass authentication and read or modify the LVS configuration via an HTTP POST request.

CVE-2013-6492 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
1043040 – (CVE-2013-6492) CVE-2013-6492 piranha: web UI authentication bypass using POST requests	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1043040
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0174
0006825: Authentication bypass in Webinterface - CentOS Bug Tracker	bugs.centos.org text/html	CONFIRM bugs.centos.org/view.php?id=6825
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0175

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	Ryan Ohara	Piranha	0.8.6	All	All	All
Application	Ryan Ohara	Piranha	0.8.6	All	All	All

cpe:2.3:a:ryan_ohara:piranha:0.8.6:*:*:*:*:*:*:*

cpe:2.3:a:ryan_ohara:piranha:0.8.6:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→