openSIS 7.4 Local File Inclusion

Authored by EgiX | Site karmainsecurity.com

Posted Jun 30, 2020

openSIS versions 7.4 and below suffer from a local file inclusion vulnerability.

tags | exploit, local, file inclusion
advisories | CVE-2020-13383
SHA-256 | e7161d7a2b2b5f3b74f9ce9373cde1c623bb264344142c67862680b20c2bfee5 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
------------------------------------------------------------------
openSIS <= 7.4 (Bottom.php) Local File Inclusion Vulnerability
------------------------------------------------------------------


[-] Software Link:

https://opensis.com/


[-] Affected Versions:

Version 7.4 and prior versions.


[-] Vulnerability Description:

The vulnerable code is located in the /Bottom.php script:

36.  if(clean_param($_REQUEST['modfunc'],PARAM_ALPHA)=='print')
37.  {
38.    $_REQUEST = $_SESSION['_REQUEST_vars'];
39.    $_REQUEST['_openSIS_PDF'] = true;
40.    if(strpos($_REQUEST['modname'],'?')!==false)
41.      $modname =
substr($_REQUEST['modname'],0,strpos($_REQUEST['modname'],'?'));
42.    else
43.      $modname = $_REQUEST['modname'];
44.    ob_start();
45.    include('modules/'.$modname);

User input passed through the "modname" request parameter is not
properly sanitized before being
used in a call to the "include()" function at line 45. This can be
exploited to include arbitrary
local files and potentially access otherwise restricted functionalities
or execute arbitrary PHP
code with the permissions of the webserver.


[-] Solution:

No official solution is currently available.


[-] Disclosure Timeline:

[04/11/2019] - Vendor notified
[04/11/2019] - Vendor acknowledgement
[10/01/2020] - Vendor contacted again asking for updates
[16/01/2020] - Vendor tried to fix the vulnerability by using
"mysqli_real_escape_string()"
[06/02/2020] - Vendor was informed about the inappropriate fix
[25/04/2020] - Version 7.4 released, vulnerability still incorrectly
fixed
[22/05/2020] - CVE number assigned
[30/06/2020] - Public disclosure


[-] CVE Reference:

The Common Vulnerabilities and Exposures project (cve.mitre.org)
has assigned the name CVE-2020-13383 to this vulnerability.


[-] Credits:

Vulnerability discovered by Egidio Romano.


[-] Original Advisory:

http://karmainsecurity.com/KIS-2020-07
```


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