

- [Home](#)
- [Vulnerabilities](#)
- [Blog](#)
- [Services](#)
- [About](#)
- [Contact](#)



SmartFoxServer 2X 2.17.0 Credentials Disclosure

Title: SmartFoxServer 2X 2.17.0 Credentials Disclosure

Advisory ID: [ZSL-2021-5627](#)

Type: Local

Impact: Exposure of Sensitive Information, Security Bypass

Risk: (3/5)

Release Date: 07.02.2021

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.

Description

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.

Vendor

`gotoAndPlay()` - <https://www.smartfoxserver.com>

Affected Version

Server: 2.17.0

Remote Admin: 3.2.6

SmartFoxServer 2X, Pro, Basic

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

Vendor Status

[29.01.2021] Vulnerability discovered.

[29.01.2021] Asked vendor about the console module, how to enable it.

[30.01.2021] No response.

[31.01.2021] Vendor contacted.

[01.02.2021] Vendor asks more details.

[01.02.2021] Sent details to the vendor.

[01.02.2021] Vendor responds.

[01.02.2021] Replied to the vendor, asking for a plan.

[03.02.2021] Vendor will fix the Credentials Disclosure. Other issues are working as expected.

[07.02.2021] Public security advisory released.

PoC

[sfs_pwd.txt](#)

Credits

Vulnerability discovered by Gjoko Krstic - [<gjoko@zeroscience.mk>](mailto:gjoko@zeroscience.mk)

References

[1] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-26550>

[2] <https://nvd.nist.gov/vuln/detail/CVE-2021-26550>

[3] <https://www.exploit-db.com/exploits/49527>

[4] <https://packetstormsecurity.com/files/161337/>

[5] <https://cxsecurity.com/issue/WLB-2021020034>

[6] <https://exchange.xforce.ibmcloud.com/vulnerabilities/196350>

[7] <https://www.tenable.com/cve/CVE-2021-26550>

Changelog

[07.02.2021] - Initial release

[10.02.2021] - Added reference [3], [4], [5], [6] and [7]

Contact

Zero Science Lab

Web: <https://www.zeroscience.mk>

e-mail: lab@zeroscience.mk

• Rete mirabilia

- **We Suggest**

- **Profiles**



-  [Site Meter](#)