

## Spyker Commerce OS Remote Command Execution

Authored by [David Brown](#), [Marcelo Reyes](#) | Site [schutzwerk.com](#)

Posted Jul 19, 2022

Spyker Commerce OS with spyker/http module versions prior to 1.7.0 suffer from a remote command execution vulnerability due to a predictable value in use.

tags | [exploit](#), [remote](#), [web](#)

advisories | [CVE-2022-28888](#)

SHA-256 | [a6d63126b4d1bdadea5938a1d895d1687c6b584abb5b278f66f4f0e3915c97bdb](#) [Download](#) | [Favorite](#) | [View](#)

### Related Files

### Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

### Change Mirror

Download

Title

=====

SCHUTZWERK-SA-2022-003: Remote Command Execution in Spyker Commerce OS

Status

=====

PUBLISHED

Version

=====

1.0

CVE reference

=====

CVE-2022-28888

Link

=====

<https://www.schutzwerk.com/en/43/advisories/schutzwerk-sa-2022-003/>

Text-only version:

<https://www.schutzwerk.com/advisories/SCHUTZWERK-SA-2022-003.txt>

Affected products/vendor

=====

Spyker Commerce OS by Spyker Systems GmbH, with spyker/http module < 1.7.0

Summary

=====

A predictable value is used to sign and verify special \_fragment URLs in Spyker Commerce OS with spyker/http module < 1.7.0. Attackers that can guess this value are able to generate valid \_fragment URLs which allow calling PHP methods, with certain restrictions. It could be demonstrated that this allows attackers to write arbitrary content to files on the file system, which, in turn, allows for execution of arbitrary PHP commands in many setups and therefore remote command execution.

Risk

=====

The vulnerability allows attackers to execute arbitrary commands on an operating system-level on systems where the Spyker Commerce OS is installed. In many cases, authentication is not necessary for successful exploitation. If attackers have already determined that Spyker Commerce OS is utilized through fingerprinting, checking for the presence of the vulnerability is trivial. With the ability to execute arbitrary commands, attacks can, for example, access customer data of the affected shop.

Description

=====

A webshop that was recently assessed for security vulnerabilities by SCHUTZWERK was found to contain a remote command execution vulnerability. The application in scope is based on a framework by Spyker -- Spyker Commerce OS. Spyker's framework, in turn, is based on Symfony[0] and/or Silex[1].

Search ...



Follow us on Twitter



Subscribe to an RSS Feed

### File Archive: November 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			

### Top Authors In Last 30 Days

Red Hat 186 files

Ubuntu 52 files

Gentoo 44 files

Debian 27 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secuR1ty 6 files

mjruczyk 4 files

George Tsimpidas 3 files

### File Tags

ActiveX (932)  
 Advisory (79,557)  
 Arbitrary (15,643)  
 BBS (2,859)  
 Bypass (1,615)  
 CGI (1,015)  
 Code Execution (6,913)  
 Conference (672)  
 Cracker (840)  
 CSRF (3,288)  
 DoS (22,541)  
 Encryption (2,349)  
 Exploit (50,293)  
 File Inclusion (4,162)  
 File Upload (946)  
 Firewall (821)  
 Info Disclosure (2,656)

### File Archives

November 2022  
 October 2022  
 September 2022  
 August 2022  
 July 2022  
 June 2022  
 May 2022  
 April 2022  
 March 2022  
 February 2022  
 January 2022  
 December 2021  
 Older

### Systems

AIX (426)  
 Apple (1,926)

Symfony and Silex both support a special `_fragment` endpoint. This feature was analyzed by Ambionics Security[2] in 2020. In their write up, the feature is described as follows:

```
One of Symfony's built-in features, made to handle ESI (Edge-Side Includes)[3], is the FragmentListener class[4]. Essentially, when someone issues a request to /_fragment, this listener sets request attributes from given GET parameters. Since this allows to run arbitrary PHP code [...], the request has to be signed using a HMAC value. [...]
```

[...] Given its importance, [the secret used for signing] must obviously be very random.

At least parts of the source code of the Spryker framework are open source and publicly accessible via GitHub. During the assessment, while certain security-sensitive parts of the source code were reviewed, it was discovered that the secret used to sign and verify `_fragment` URLs is static and predictable. The secret is set to `md5(__DIR__)` in the PHP file `HttpFragmentServiceProvider.php`[5] and in two different `HttpConfig.php`[6][7] files.

`__DIR__` is a built-in "magic constant" in PHP[8] and it corresponds to "the directory of the file". It is not entirely clear, which of these PHP files is actually included and loaded by the Spryker framework. However, it is assumed that the file `http/src/Spryker/Shared/Http/HttpConfig.php` is the culprit.

Guessing the secret  
^^^^^^^^^^^^^^^^^^^^

In order to gain a better understanding of the vulnerability, SCHUTZWERK set up a local Spryker development instance with a demo shop[9] in order to allow for more in-depth debugging.

By inspecting the source code and adding appropriate debug statements, the secret was identified as `e3ae11e53f7c3d72da08784b9af763f9`. This corresponds to the MD5 sum of the path `/data/shop/development/current/vendor/spryker/http/src/Spryker/Shared/Http:`

```
$ echo -n '/data/shop/development/current/vendor/spryker/http/src/Spryker/'\
'Shared/Http'| md5sum
e3ae11e53f7c3d72da08784b9af763f9 -
```

The proof-of-concept script `find_secret.py`[10] was developed in order to automate the process of identifying the secret based on a list of known Spryker paths. The script was executed as follows against the local development instance and correctly identified the static secret:

```
$ python3 find_secret.py --path-list known_spryker_paths.txt \
http://www.de.b2b-demo-shop.local/_fragment
[-] http://www.de.b2b-demo-shop.local/_fragment
2c03fc8fac1ff5204b56d4dbf879a3fc
[-] http://www.de.b2b-demo-shop.local/_fragment
f71e9665ffe0a0e3b54bbe7c2642d466
[-] http://www.de.b2b-demo-shop.local/_fragment
faf0d063ad6adf3776d59bc55a17aa5f
[+] http://www.de.b2b-demo-shop.local/_fragment
e3ae11e53f7c3d72da08784b9af763f9

(/data/shop/development/current/vendor/spryker/http/src/Spryker/Shared/Http)
```

This verification step does not require authentication in the default configuration. The script generates `_fragment` URLs based on a provided list of paths and detects whether the server views these URLs as valid (correctly signed) or not. This distinction is made based on different observations (e.g. status code, response content, etc.).

The same script was then executed against the customer's instance:

```
$ python3 find_secret.py --path-list known_spryker_paths.txt \
[CUSTOMER_DOMAIN]/_fragment
[-] [CUSTOMER_DOMAIN]/_fragment e3ae11e53f7c3d72da08784b9af763f9
[-] [CUSTOMER_DOMAIN]/_fragment faf0d063ad6adf3776d59bc55a17aa5f
[-] [CUSTOMER_DOMAIN]/_fragment 8399015c0dbbf2162983fb7ad0ea6a9a
[-] [CUSTOMER_DOMAIN]/_fragment 8baff412797b1ddd80cd968e7446aa06
[...]
[-] [CUSTOMER_DOMAIN]/_fragment 2c03fc8fac1ff5204b56d4dbf879a3fc
[-] [CUSTOMER_DOMAIN]/_fragment d6de8df0b4ad55b15f198e06142dd0e6
[-] [CUSTOMER_DOMAIN]/_fragment d6de8df0b4ad55b15f198e06142dd0e6
[+] [CUSTOMER_DOMAIN]/_fragment 9c15f40d8e5610e89caf6f9b7a97be3b
(/data/srv/yves/www/vendor/spryker/http/src/Spryker/Shared/Http)
```

In this case, the identified secret `9c15f40d8e5610e89caf6f9b7a97be3b` corresponds to the path `/data/srv/yves/www/vendor/spryker/http/src/Spryker/Shared/Http`.

The installation path of the application can of course vary greatly between installations. However, if customers use the official Docker guide provided by Spryker, it is likely that they will use the paths utilized in the examples and thus share a common installation path.

Even if this is not the case, customers might share installation paths between multiple environments (development, production). A compromise of one installation would therefore make a compromise of the other installations likely.

Signing URLs  
^^^^^^^^^^^^

In addition to the secret, a URL must be passed to the HMAC function to form the signature. However, in both instances of the vulnerability that were discovered during the assessment, the URL was the same as the external URL. This might be true for all Commerce OS installations.

Intrusion Detection (866)	BSD (370)
Java (2,888)	CentOS (55)
JavaScript (817)	Cisco (1,917)
Kernel (6,255)	Debian (6,620)
Local (14,173)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,390)	Gentoo (4,272)
Perl (1,417)	HPUX (878)
PHP (5,087)	iOS (330)
Proof of Concept (2,290)	iPhone (108)
Protocol (3,426)	IRIX (220)
Python (1,449)	Juniper (67)
Remote (30,009)	Linux (44,118)
Root (3,496)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,768)	OpenBSD (479)
Shell (3,098)	RedHat (12,339)
Shellcode (1,204)	Slackware (941)
Sniffer (885)	Solaris (1,607)
Spoof (2,165)	SUSE (1,444)
SQL Injection (16,089)	Ubuntu (8,147)
TCP (2,377)	UNIX (9,150)
Trojan (685)	UnixWare (185)
UDP (875)	Windows (6,504)
Virus (661)	Other
Vulnerability (31,104)	
Web (9,329)	
Whitepaper (3,728)	
x86 (946)	
XSS (17,478)	
Other	



Solution/Mitigation  
=====

1. Update spryker/http module to version 1.7.0  
2. Configure SPRYKER\_ZED\_REQUEST\_TOKEN environment variable with a long, random and secure string

Disclosure timeline  
=====

2022-04-07: Vulnerability discovered  
2022-04-07: Initial contact with vendor  
2022-04-08: Vulnerability reported to vendor  
2022-04-08: CVE-2022-28888 assigned by MITRE  
2022-04-11: Vendor notifies customers about vulnerability, releases patch  
2022-04-26: Requested update from vendor  
2022-05-05: Requested update from vendor  
2022-06-20: Notified vendor of intention to publish advisory on 2022-06-30  
2022-06-22: Vendor confirms that customers were notified about the vulnerability  
2022-07-12: Advisory published by SCHUTZWERK

Contact/Credits  
=====

The vulnerability was discovered during an assessment by David Brown and Marcelo Reyes of SCHUTZWERK GmbH.

References  
=====

[0] <https://symfony.com>  
[1] <https://github.com/silexphp/Silex>  
[2] <https://www.ambionics.io/blog/symfony-secret-fragment>  
[3] [https://en.wikipedia.org/wiki/Edge\\_Side\\_Includes](https://en.wikipedia.org/wiki/Edge_Side_Includes)  
[4] <https://github.com/symfony/symfony/blob/ac236517cc8925110d2ec9c35cfdb682a7b82f06/src/Symfony/Component/HttpKernel>  
[5] <https://github.com/spryker/silexphp/blob/94d2afc9b1ed9662193985cad1ba47da33bdc80d/src/Silex/Provider/HttpFragmer>  
[6] <https://github.com/spryker/http/blob/56313eaff6594821849846d1b93e0b7eba9a09b6/src/Spryker/Shared/Http/HttpConfig>  
[7] <https://github.com/spryker/spryker-core/blob/88ab823143b5521b4e1bb1b930321ec39eb4ec1e/Bundles/Http/src/Spryker/Shared/Http/HttpConfig.php#L29>  
[8] <https://www.php.net/manual/en/language.constants.magic.php>  
[9] <https://docs.spryker.com/docs/scos/dev/setup/installing-spryker-with-development-virtual-machine/installing-spryker-with-devvm-on-macos-and-linux.html>  
[10] [https://www.schutzwerk.com/en/43/assets/advisories/find\\_secret.py](https://www.schutzwerk.com/en/43/assets/advisories/find_secret.py)

Disclaimer  
=====

The information provided in this security advisory is provided "as is" and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible. The most recent version of this security advisory can be found at SCHUTZWERK GmbH's website ( <https://www.schutzwerk.com> ).

--  
SCHUTZWERK GmbH, Pfarrer-WeiB-Weg 12, 89077 Ulm, Germany

Phone +49 731 977 191 0  
Fax +49 731 977 191 99  
Mobile +49 171 337 2701

advisories@schutzwerk.com / [www.schutzwerk.com](https://www.schutzwerk.com)

Geschäftsführer / Managing Directors:  
Jakob Pietzka, Michael Schäfer

Amtsgericht Ulm / HRB 727391

◀

▶

[Login](#) or [Register](#) to add favorites



© 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