intruder

Scan Summary: **Fraxion Pty Ltd**

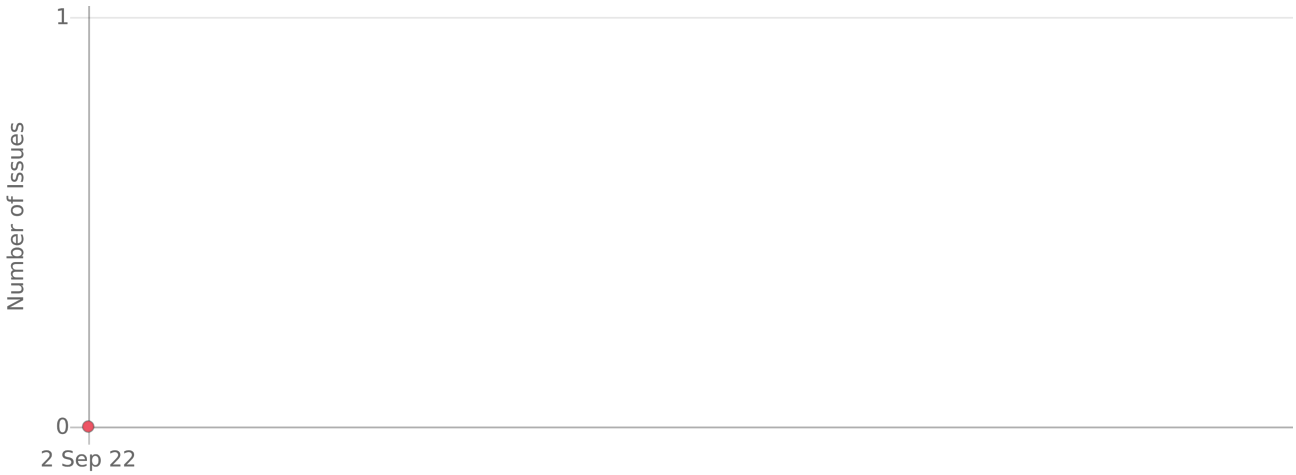
2 September 2022

All clear

No issues were discovered that could lead to or increase the chances of a breach. While this is a good position to be in today, new weaknesses are discovered daily, and changes are often made to systems that could reduce their security. Make sure to continue using ongoing security services to monitor your risk.

0	0	0	0
Critical issues	**High** issues	**Medium** issues	**Low** issues

Exposure over time



Differences since last assessment

New issues discovered		Previous issues remediated		Direction of travel
Critical	0	Critical	0	▲▼ 0
High	0	High	0	▲▼ 0
Medium	0	Medium	0	▲▼ 0
Low	0	Low	0	▲▼ 0

What we checked

Total checks	Targets	Issues discovered
11,443	**1**	**0**

Here are some examples of what we checked your targets and their reachable webpages for.

Vulnerable software & hardware

- Web servers, e.g. Apache, Nginx
- Mail servers, e.g. Exim
- Development software, e.g. PHP
- Network monitoring software, e.g. Zabbix, Nagios
- Networking systems, e.g. Cisco ASA
- Content management systems, e.g. Drupal, Wordpress
- Other well-known weaknesses, e.g. 'Log4Shell' and 'Shellshock'

Web Application Vulnerabilities

- Checks for multiple OWASP Top Ten issues
- SQL injection
- Cross-site scripting (XSS)
- XML external entity (XXE) injection
- Local/remote file inclusion
- Web server misconfigurations
- Directory/path traversal, directory listing & unintentionally exposed content

Attack Surface Reduction

Our service is designed to help you reduce your attack surface and identify systems and software which do not need to be exposed to the Internet, such as:

- Publicly exposed databases
- Administrative interfaces
- Sensitive services, e.g. SMB
- Network monitoring software

Information Leakage

Checks for information which your systems are reporting to end-users which should remain private. This information includes data which could be used to assist in the mounting of further attacks, such as:

- Local directory path information
- Internal IP Addresses

Encryption weaknesses

Weaknesses in SSL/TLS implementations, such as:

- 'Heartbleed', 'CRIME', 'BEAST' and 'ROBOT'
- Weak encryption ciphers & protocols
- SSL certificate misconfigurations
- Unencrypted services such as FTP

Common mistakes & misconfigurations

- VPN configuration weaknesses
- Exposed SVN/git repositories
- Unsupported operating systems
- Open mail relays
- DNS servers allowing zone transfer

As a **Pro** plan customer, you also have access to:

Emerging threats

The time between new vulnerabilities emerging and hackers exploiting them is now days, not weeks. For organizations who need a more mature approach to cyber security, our emerging threat scans detect critical threats to your systems without waiting for the next monthly check.

Internal checks

Your internal systems can also be hacked with a little extra effort, e.g. by an email or web page link that exploits known unpatched software or an employee's device. Our agent-based scanner can be installed on each machine you want to protect.

Scan Info

Targets included in this scan

swift.spendmanagement.com

Scan timings

This scan ran from 02 Sep 2022 11:15 to 02 Sep 2022 12:04.