intruder

Scan Summary: **Apply Financial**
Additional target: **apps.applyfinancial.co.uk**
27 July 2020

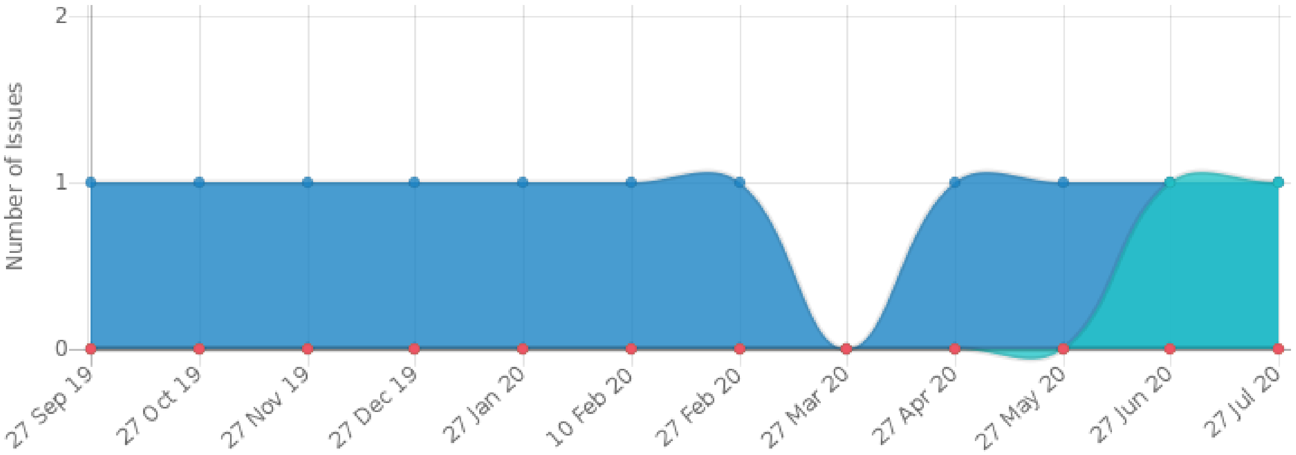
Medium

Threat Level

Medium severity issues are unlikely to lead to a breach, as they generally require a level of skill or resource available to only the most highly capable attackers, such as nation states or organised cyber crime groups. Medium severity issues should be fixed if the business faces a significant threat from being targeted by such skilled attackers, ideally within 90 days.

0	0	1	1
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 you for

You're on our Verified plan, which means all the targets included and their reachable webpages were checked for over 10,000 weaknesses including:

✓ **Vulnerable Software**

Thousands of checks for known weaknesses in a huge variety of software and hardware, such as: *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), as well as other well-known weaknesses, such as 'Shellshock'*

✓ **Web Application Vulnerabilities**

Includes but is not limited to: *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*

✓ **Common Mistakes & Misconfigurations**

Checks for a wide range of misconfigurations, common mistakes and security best practices. These include: *VPN configuration weaknesses, exposed SVN/git repositories, unsupported operating systems, open mail relays, DNS servers allowing zone transfer*

✓ **Encryption Weaknesses**

Weaknesses in SSL/TLS implementations, such as: *'Heartbleed', 'CRIME', 'BEAST', and 'ROBOT', weak encryption ciphers, weak encryption protocols, SSL certificate misconfigurations, unencrypted services such as FTP*

✓ **Attack Surface Reduction**

Our service is designed to help your organisation reduce its 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, such as 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, and internal IP addresses.*

Those are the checks that were made for this report. However, your service with us also includes:

✓ **Monthly Checks**

On average, more than 20 new vulnerabilities are discovered every day. A hacker may only need ***one*** of these to breach your systems. The Verified plan includes monthly checks for the latest weaknesses which may affect your systems, and ensures any recent changes haven't compromised your security.

✓ **Emerging Threats**

The time between new vulnerabilities emerging and hackers exploiting them is now days, not weeks. For organisations 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.

✓ **Expert Analysis**

Automated tools can identify the majority of issues, but there's always a chance a human could find more. Our manual checks are performed by expert penetration testers on a rolling monthly basis, so you get the quality of a penetration test, on a more regular schedule.

Issue Summary

Impact	Issue details
Medium	JQuery Version In Use Contains Known Vulnerabilities Number of occurrences: 1
Low	Weak TLS Protocol Version Supported Number of occurrences: 1

Issues

JQuery Version In Use Contains Known Vulnerabilities

Description

The version of JQuery in use contains a number of known security vulnerabilities which could be used to compromise the system or affect its availability.

JQuery is a popular JavaScript library used in web development.

Remediation Advice

Upgrade the version of JQuery in use to the latest available supported version.

Occurrences

	Version	First seen
apps.applyfinancial.co.uk : 443 (tcp)	2.1.0	27 Jun 2020 01:28

Weak TLS Protocol Version Supported

Description

A service on the host was found to support a weak version of the 'Transport Layer Security' (TLS) encryption protocol. TLS is used to encrypt data in transit between a client and server, and older versions of the protocol (TLS 1.0 and TLS 1.1) have been deprecated in favour of the more secure, newer versions of the protocol (TLS 1.2, TLS 1.3). If an attacker is able to intercept the communications between the client and the server, they would theoretically be able to decrypt this communication.

Please note that the complexity and mathematics behind the attack are non-trivial and make it infeasible for all but the most highly skilled and resourced attackers.

Remediation Advice

The most secure versions of the TLS encryption protocol are TLS 1.2 and TLS 1.3. Where possible, TLS 1.0 and TLS 1.1 should be disabled entirely to avoid the possibility of an attacker downgrading the encryption protocol in use to one of these older, insecure versions.

Occurrences

	First seen
apps.applyfinancial.co.uk : 443 (tcp)	27 May 2019 01:17

Raw Reconnaissance Data

Target (IP and Hostnames)	Port	Protocol	Service	Service info
195.157.4.130 apps.applyfinancial.co.uk	443	tcp	http	nginx
	80	tcp	http-proxy	Varnish http accelerator

Scan Info

Targets included in this scan

apps.applyfinancial.co.uk

Scan timings

This scan ran from 27 Jul 2020 01:04 to 27 Jul 2020 02:05.

About Intruder

Intruder Systems Ltd is an independent security advisory company, specialising in providing continuous security monitoring for internet-facing web applications and infrastructure.

Intruder consultants have previously worked for Big Four professional services firms, as well as specialist technical security consultancies. This background has afforded Intruder industry-leading technical skills combined with thorough professionalism. Intruder consultants have delivered work for government agencies, international financial institutions, and global retail giants.

Intruder aims to deliver the highest calibre of security assessments in the industry, with a focus on technical excellence, risks presented in the context of realistic scenarios, and delivered with the utmost quality.

Intruder is Cyber Essentials certified.

Professional Membership

Intruder is a member of the Cyber-security Information Sharing Partnership.

The Cyber-security Information Sharing Partnership (CiSP), part of CERT-UK, is a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.

Intruder is a partner of the Cyber Growth Partnership.

The Cyber Growth Partnership (CGP) is a group composed of representatives from UK industry, government and academia. The GCP provides oversight and gives strategic guidance to the Government on supporting the development of the UK cyber security ecosystem.

Credentials

GCHQ Cyber Accelerator Alumni

BT SME Award 2017 – "Securing the Nation": Cyber Security category

Finalist – UK's Most Innovative Small Cyber Security Company 2016 – DCMS & techUK

CyLon Accelerator Alumni

intruder

🌐 www.intruder.io ✉ contact@intruder.io 🐦 intruder_io