Info Flash
Security Enhancement (TLS)

Date: 22/01/2018

A team of researchers has announced that Transport Layer Security (TLS) stacks from at least 8 different vendors are vulnerable to a well-known 19-year-old protocol flaw, Return of Bleichenbacher's Oracle Threat hence ROBOT.

Successful exploitation of this vulnerability allows attackers to perform cryptographic operations using the private key configured on the vulnerable server. This means that an attacker could decrypt previously recorded sessions established with an RSA key exchange. Attackers could also carry out a signature attack within the duration of a TLS handshake resulting in a full man-in-the-middle attack.

The most complete known remediation thus far is to disable RSA encryption-based key exchange modes where possible. This guarantees protection against known and unknown vulnerabilities with a minimal impact on HTTPS client compatibility.

Fundsquare positions the integrity and security of client's information going through our infrastructure or stored in our referential at the very top of its priorities.

As a result we'd like to inform that Fundsquare is quickly enhancing the security of its applications and the related communication channels or interfaces, while disabling RSA key exchange as of Monday 22nd January 2018.

Note -> Technical information (supported key exchange) :

```
# TLS 1.0
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
# TLS 1.1
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
# TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

In case of any furhter questions, please do not hesitate to contact us as the provided contact details.

Thank you for using our services and the trust you have in us.

Kind regards,

Helpdesk Team

Phone +352 28 370 211
helpdesk@fundsquare.net