KMBL Security

Factoring Attack on RSA-EXPORT Keys (FREAK)

CVE-2015-0204

Use License

- **You are free to:**
  - **Share** — copy and redistribute the material in any medium or format
  - **Adapt** — remix, transform, and build upon the material
- The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

- **Attribution** — You must give **appropriate credit**, provide a link to the license, and **indicate if changes were made**. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **NonCommercial** — You may not use the material for **commercial purposes**.
- **No additional restrictions** — You may not apply legal terms or **technological measures** that legally restrict others from doing anything the license permits.
- **Notices:**
- You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable **exception or limitation**.
- No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as **publicity, privacy, or moral rights** may limit how you use the material.

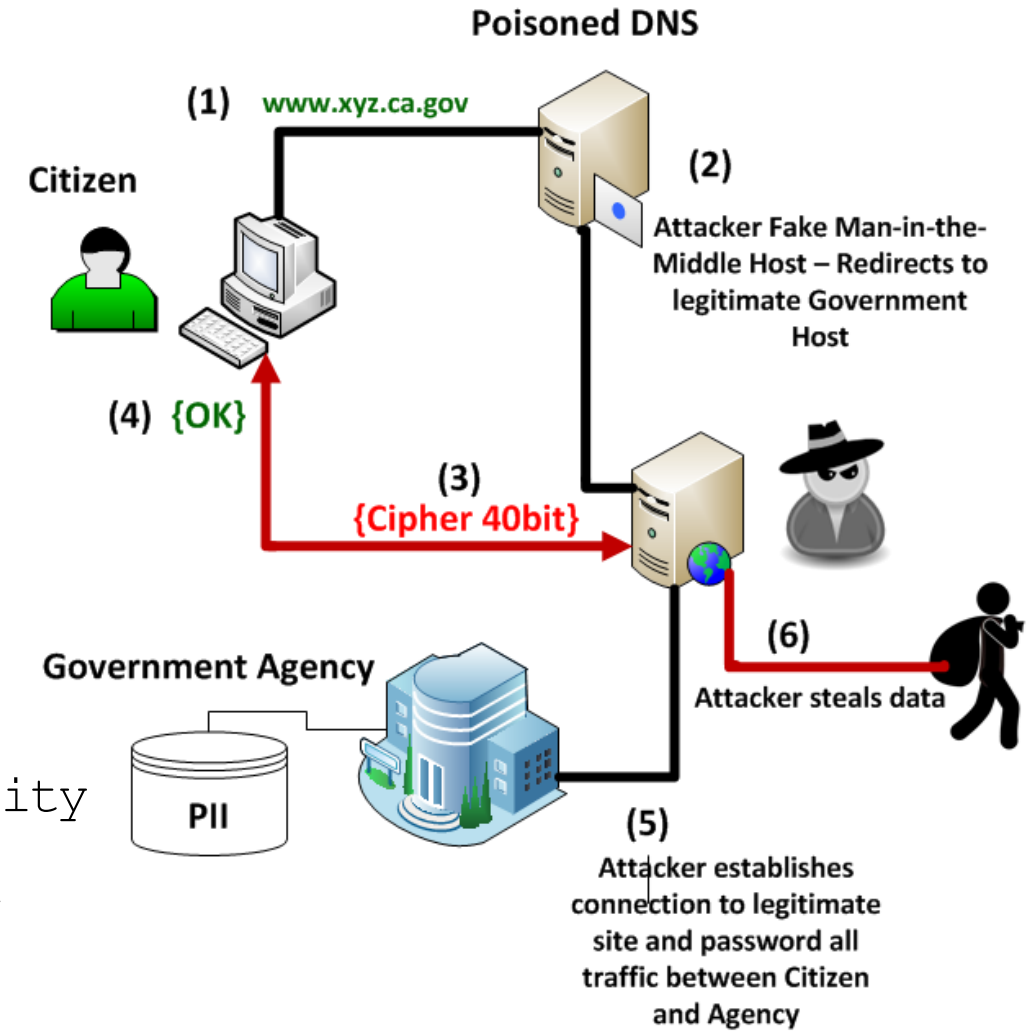
Agenda

- Related Risks to SSL
- Issue – Background
- CVE Overview
- Potential Impacts to Entities
- Detection Mechanisms
- Risk Mitigations

Related SSL Risk

- **Cipher Agreement:**
  The protocol is designed to allow for encryption at the highest agreed upon mutually supported common cipher
  - **Assumptions:**
    - Highest common cipher is transmitted
    - Processing power required to break the agreed upon cipher is computationally unfeasible within the time of data usability

- **Issue:** What is one of more of these assumptions in *invalid*?



Why this Risk Exists

- Post World War II – Allies recognize value of cryptography
  - Implications: Tool for secrecy and weapon to ease drop assumed private communications
- Export restrictions implemented to prevent U.S. cryptography advances from use by hostile countries
- Cryptography placed on the U.S. Munitions Restricted Export List
  - Auxiliary Military Technology
- Internet boom drove international encryption compatibility requirements
- All browsers included “Export” ciphers to support international commerce
- In 2000, export restrictions
- Backwards compatibility in browsers remained

CVE Overview

National Cyber Awareness System

Vulnerability Summary for CVE-2015-0204

Original release date: 01/08/2015

Last revised: 03/26/2015

Source: US-CERT/NIST

Overview

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) (legend)

Impact Subscore: 2.9

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized modification

Manifests in Three Locations:

- Web Servers
- Web Clients
- **Mobile Clients**

Server CVE(s):

- CVE-2015-1637 (Microsoft)
- CVE-2014-3572 (OpenSSL)

Client CVE

CVSS Score of 8.6 is rated as High – defined as: "The vulnerability can be exploited by automated code…".

Mobile OS's:

Dependent on carrier deployment

Potential Impacts to Entities

The following potential impacts exist for vulnerable sites:

- Risk to Confidentiality of Restricted Data
- Data Exfiltration by unauthorized malicious actors
    - Leaked Data posted via pastebin, etc…
- Data Breach (PII, PCI, PHI, etc…)
- Potential for Credential Theft
- Potential for Unauthorized Access

Detection Mechanisms

- **3rd party Websites**
  - https://tools.keycdn.com/freak
  - https://www.ssllabs.com/ssltest/
  - *Always judge the reliability of the site and know the information disclosure policies of 3rd party sites prior to their use!*

- **Open Source Tools:**
  - NMAP – SSL-Enum-Cipher NSE Script
    - Can be scripted to eliminate noisy results
    - Results are controlled by agency (vs 3rd party exposure)
    - Can be run on Internet assets to detect Insider risks
  - SSLScan

- **Commercial Tools:**
  - Qualys
  - Nessus
  - Netsparker

** KMBL does not endorse any specific tools, these are just listed for technical reference*

Sample Script - NMAP

Loop Multiple Sites, Filters Results "Weak/Broken"

Writes findings to Text file …

```
#!/bin/bash
# automation of nmap --script ssl-enum-ciphers script that accepts a list of domains and writes each result to file
# By: K. Foster 3/22/2015

# prerequsite:  Generate a text file with one subdomain per line (e.g. intranet.acme.com ) as an input

echo "Input the file name of the target subdomain list: "
read loopfile
echo
echo
for sdt in $(cat $loopfile);do
    echo " [+] Starting "$sdt
    echo $sdt" Site Results: " >> target-results.txt
    echo " " >> target-results.txt
    nmap --script ssl-enum-ciphers -p 443 $sdt | grep -E 'weak|broken' >> target-results.txt
    echo "   >> " $sdt " Results completed"
    echo " " >> target-results.txt
done
```

- Script initiates an SSL handshake and enumerates the supported ciphers, one at a time - This Script can be noisy!
- No warranty or support is provided for this script.

Risk Mitigations

- Server Common Server Platforms:
  - Microsoft:
    - KB MS15-031 – Vulnerability in Schannel Could Allow Security Feature Bypass
  - Apache:
    - Security Advisory 20150108
    - Mitigation steps:
      - ***Locate httpd ssl.conf file***
      - ***Modify the SSLCipherSuite setting – HIGH: !aNULL:!MD5:!EXP***

Prior to Implementing ALWAYS evaluate the impact on current business operations!

- *If 3rd party tools / software is impacted, contact vendor support for security patches and assistance*
- *If vendor will not / can not fix, then a NEW Risk Acceptance is required by Agency Director*

Questions

Our Challenge as Cybersecurity Professionals:

Attacks only get better with time