POODLE Bug Advisory (CVE-2014-3566)

MSS-SIEM
Prepared By: Accuvant MSS / Revision Number: 1.0
Date: 10/15/2014

Table of Contents

Technical Summary

Overview of POODLE Attack

POODLE (Padding Oracle on Downgraded Legacy Encryption) is an attack targeting SSLv3, a legacy SSL protocol that is over 15 years in age. The SSLv3 protocol has recently been found to contain numerous vulnerabilities, including Browser Exploit Against SSL/TLS (BEAST), which could result in disclosure of plaintext data. The POODLE attack in this case could yield access to "secure" HTTP session cookies or other authorization tokens present in HTTP headers. The disclosed information could be used to perform a session hijacking attack against the user and a specific application.

The POODLE attack targets an end-user by forcing a downgrade of an SSL/TLS connection SSLv3. The attack requires a man-in-the-middle (MITM) or other "hooks" to effectively deliver the attack. This requires physical proximity (LAN/wireless) to the user or access to upstream traffic to perform a MITM attack. At this time no public demonstrations of the attack or simple exploit code exist that would enable an attacker to easily take advantage of this. Accuvant MSS rates this vulnerability at a medium level of severity due to the complexity required for exploitation.

Impact

POODLE is considerably less severe than the Heartbleed vulnerability simply due to how complicated it is to exploit. POODLE is an indirect attack that requires MITM or "hooking" a user with JavaScript for delivery. Heartbleed is a direct attack vector that is very easy to deliver and exploit resulting in all the information that could be disclosed in a POODLE attack and more.

The end impact of this attack is generally access to live session cookies that could be used for session hijacking. The attacker would need to perform the attack and maintain the "hook" long enough to pull down the full decrypted session cookie, which could take tens of thousands of requests. The user would also need to keep the browser open for the entire duration of the attack and the session cookies would need to maintain consistency throughout the session. If the session value rotates during the attack, the attacker will have to start over.

Updates

None updates at this time.

Affected Versions and Products

Every single web server that allows SSLv3 is potentially vulnerable. This means every single vendor and also "HTTPS endpoints" such as SSL-VPN that use HTTPS from every vendor. There is no patch yet from any of the major vendors. This means the following products are likely affected:

- SSL-VPN devices including Juniper, F5 and Cisco
- Microsoft IIS – All versions
- Apache Web Server – All versions and all software derived from Apache
- Oracle HTTP server
- Oracle Weblogic
- IPlanet
- IBM HTTP Server
- Apache Tomcat
- LightHTTPD
- NGINX
- Zope
- Zeus

- WEBrick
- THTTPD
- Resin
- LiteHTTPD
- F5 Load Balancers
- Services with “HTTPS” interface points such as instant messaging servers
- “Home Grown” HTTP servers based on python, perl and other scripting languages

The vulnerability **DOES NOT** affect the following:

- Sites that force TLS 1.X and explicitly disallow SSLv3 explicitly
- End-user browsers that do not allow SSLv3 explicitly

Determining Vulnerability

A number of tools have been developed to address this vulnerability including both online tools and standalone tests.

Commercial Vulnerability Scanning Tools

At this time no scanning vendors have released an official signature update to test for this specific vulnerability by name. Commercial scanning tools can be used to identify systems that support SSLv3 using the standard SSL/TLS test cases. Any system or service supporting SSLv3 at this time should be considered vulnerable.

SSLLabs.com

The SSLLabs.com suite provides a free, web-based mechanism for testing for the heartbeat vulnerability and a number of other SSL related issues.

NMAP

NMAP introduced a SSL cipher enumeration test NSE check to enumerate supported SSL protocols and ciphers. The output in this case is a bit difficult to parse but NMAP is a great tool for testing multiple sites.

```
# turn off pings, turn off dns resolution pull version banners, run the test script, output in all formats and pull in a
# list of targets
nmap –T3 –n –vvv –PN -sV –open --script=ssl-enum-ciphers –web-xml –oA POODLE_SCAN –iL targets.txt
```

Keep in mind the sample output in this case lists some of the ciphers as strong despite the deficiency in all SSLv3 implementations. Any mention of SSLv3 indicates vulnerability in this case.

```
PORT    STATE SERVICE REASON
443/tcp open  https   syn-ack
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_RC4_128_MD5 - st
|       TLS_RSA_WITH_RC4_128_SHA - st
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Recommendations

Patching

At this point in time no patches are available to address the issue from any vendor.

Workaround

Disable SSLV3 Support Explicitly
By completely eliminating SSLv3 from the environment. All organizations should do this any way because SSL in particular is being looked at in depth by attackers. Many of the recent vulnerabilities in SSL are mitigated by using modern versions of the TLS protocol in conjunction with perfect forward secrecy (PFS). The chance for issues with backwards compatibility is quite low.

There are other workarounds using TLS fallbacks but this is complex and potentially error prone. The existing fallback measures are only in draft form and not recommended for production environments.

Microsoft IIS

Disable SSL 3.0 and enable TLS 1.0, TLS 1.1, and TLS 1.2 in Group Policy
You can disable the SSL 3.0 protocol that is affected by this vulnerability. You can do this by modifying the "Turn Off Encryption Support Group Policy Object"

1. Open Group Policy Management.
2. Select the group policy object to modify, right click and select Edit.
3. In the Group Policy Management Editor, browse to the following setting: Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Explorer Control Panel -> Advanced Page -> Turn Off Encryption Support
4. Double-click the Turn off Encryption Support setting to edit the setting.
5. Click Enabled.
6. In the Options window, change the Secure Protocol combinations setting to "Use TLS 1.0, TLS 1.1, and TLS 1.2".
7. Click OK.

Many web servers are derived from Apache and use an Apache like syntax. Use this as a template for remediation.

Apache / Apache Derivatives

```
# Intermediate configuration, tweak to your needs
SSLProtocol all -SSLv2 -SSLv3

# Recommended cipher suites for perfect forward secrecy
SSLCipherSuite  ECDHE-RSA-AES256-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-
GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-
AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-
RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:
AES:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK
SSLHonorCipherOrder on
SSLCompression  off
```

NGINX

```
server {
listen 443;
ssl on;
# Diffie-Hellman parameter for DHE ciphersuites, recommended 2048 bits
# Intermediate configuration. tweak to your needs.
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-
SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-
AES256-SHA:ECDHE-ECDSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK';
ssl_prefer_server_ciphers on;

# Enable this if your want HSTS (recommended)
add_header Strict-Transport-Security max-age=15768000;
}
```

IE6 Backward Compatibility

Most sites on modern versions of IIS, NGINX, F5 load balancers and apache have support for TLS enabled now but not required. For example, Firefox published a statistic that only 0.3% of all web traffic is actually using SSLv3 at this point. This means sites that explicitly disallow TLS 1.X which is extremely rare and the chances of an issue arising due to SSLv3 being disabled is extremely low. IE 6.0 is the only recent browser that does not support TLS 1.0 and this is a deprecated product.

Here are some stats on how many users still use IE6 and SSLv3:

- https://www.modern.ie/en-us/ie6countdown
- https://blog.cloudflare.com/sslv3-support-disabled-by-default-due-to-vulnerability/ 0.09% of all users use SSLv3

Keep in mind that VERY few enterprise customers actually still use IE6 and VERY few home users actually use IE because of more popular alternatives such as Chrome and Firefox. IE6 is also commonly linked to legacy versions of windows that are at the end of their support life. Firefox and Chrome will likely eliminate support out of the box for SSLv3 based on recent articles and the sheer number of vulnerabilities identified in the last 18 months in these protocols.

Implement Perfect Forward Secrecy (PFS)

PFS can help minimize the damage in the case of a secret key leak by making it more difficult to decrypt already-captured network traffic. Technically this does not address POODLE; however the workarounds required by POODLE are an excellent opportunity to improve the overall security of SSL/TLS in the environment with minimal impact to users. Ticket keys may only be regenerated when a web server is restarted. The SSLLabs.com SSL Best Practices Guide provides a detailed set of recommendations around implementing PFS on common platforms.

Monitoring/Detection

The ability to detect the attack depends on a number of factors like log verbosity and also the ability to decrypt traffic by IDS. The good news is there are no known public exploits. Much like BEAST, which was identified by the same researchers, there is no point and shoot exploit code included with the advisory.

Expect signatures very soon from security vendors but in the meantime consider identifying anomalies in SSL/TLS negotiations for spikes in SSLv3 traffic. Given the rarity of clients connecting using SSLv3 and the default cipher list of modern browsers and default configuration of most web servers, it is possible to monitor for an excessive number of SSLv3 requests. Using the attack it takes 256 SSL 3.0 requests for each BYTE of data. In short, by establishing a baseline for SSLv3 traffic in the environment it can be determined if an attack is potentially in progress against an end-user.

Accuvant MSS Recommendations

Strategic Recommendations

To ensure thorough mitigation Accuvant strongly recommends the following additional steps:

- Explicitly Disable SSLv3 and Require TLS 1.X with strong ciphers and PFS.
  - Major browser vendors will be disabling SSLv3 support by default in future releases including Chrome, Firefox and Safari.
  - Disabling SSLv3 will only affect an extremely small subset of users on IE6. Most of these users will have an alternative browser such as Chrome or Firefox available.
  - Requiring SSLv3 will not affect smartphones developed after 2009.
  - Prioritize recommendations for addressing external systems first since they are by far the most likely to be targeted.
- Avoid “Man-in-the-Middle” Opportunities
  - Avoid using insecure public networks that could be used to perform a MITM attack to inject JavaScript “hooks” into the contents of a page.
  - Utilize secure DNS resolution where possible to prevent DNS poisoning attacks that could redirect a user to a malicious site.
  - Consider using cellular hotspots or Mifi in favour of public Wi-Fi to avoid attacks.
  - Implement certificate pinning controls in mobile applications and end-user systems using tools such as EMET to detect man-in-the-middle attacks.
  - Implement secure VPN solutions that force all traffic over the tunnel to protect data in transit with secure SSL protocols (TLS 1.x) and strong encryption with PFS. This assumes the VPN server is also not vulnerable to the same attack.
  - Implement secure, cloud-based content filtering that forces all traffic over the tunnel to protect data in transit with secure SSL protocols (TLS 1.x) and strong encryption with PFS.
  - Educate end-users to spot MITM attacks with scenarios showing SSL certificate error messages.
- Patch Services
  - Update any services and applications using SSL and any HTTP servers in the environment. This include mail servers and most external facing services.
  - Update any services in the environment that actively use HTTPS including appliances, web based management consoles etc.
- Prevent and Detect Session Hijacking
  - Regularly rotation session cookies in an application limits the window a disclosed session cookie is valid thus complicating the attack.
  - Implementing session to IP binding for end-user sessions will prevent session hijacking if an attacker is accessing the site from a separate IP space although this is unlikely due to the required proximity for a MITM attack.
  - Alert the user and deauthorize the oldest session when multiple simultaneous logins are detected. Multiple simultaneous logins are prohibited by default, but may be enabled by changing a configuration setting.
  - Terminate session and send security SNMP trap or other configurable message if User-Agent string or other client fingerprinting changes.

References and Disclaimer

1. https://www.openssl.org/~bodo/ssl-poodle.pdf
2. https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Revisions

Release Version:	1.0 – Initial Release
Date:	10/15/2014
Summary of Changes:	Initial release