SSL: A False Sense of Security?

How the Tenable Solution Restores SSL Effectiveness and Mitigates Related Threats

White Paper

INTRODUCTION – THE SSL SCENARIO

The Secure Sockets Layer (SSL) protocol has become the backbone of secure network communications, protecting everything from employee remote access, email, file transfer, and systems administration traffic to all of an organization's e-commerce transactions. But is the security SSL/TLS provides real, or just an illusion?

This is a fair question considering the surprising results of SSL-focused scans of top web sites. The finding revealed that approximately 85% of the world's most popular sites are routinely determined to be "insecure" due to weak SSL configurations and/or susceptibility to known SSL exploits. For example, more than one third of evaluated sites support the use of weak encryption ciphers[1].

While SSL is easy to deploy, and therefore very commonly used, don't assume that it "just works". "Just working" is not the same as actually being implemented and used in a trustworthy and truly secure manner. The following are the most important characteristics and potential issues pertaining to SSL that are often overlooked.

SSL is about more than just encryption. SSL is most widely recognized for its core encryption capabilities. By providing confidentiality and integrity for network communications between two parties it ensures that private content cannot be viewed by other parties and that it has not been tampered with during transmission. Under the surface, however, SSL certificates serve another important purpose: authentication. In this capacity, they are essentially the basis for trust in a transaction, as they provide assurance to a remote party that the destination host is in fact who it says it is.

The trouble comes when organizations have certificates that are not properly configured in this regard – for example, because they are unsigned, self-signed, or expired. In such cases, encryption will continue to be provided; it's just that the connecting party can't be certain who is at the other end. This might be acceptable for internal use cases, such as an intranet or applications running in a test and development network. However, for public-facing services, organizations run the risk of users abandoning their sessions when they're confronted with ominous sounding "certificate warnings" from their browsers. Some browsers will even prevent/drop sessions automatically (i.e., without warning) when presented with these types of trust-related issues.

SSL is easy to "mis-configure". A big part of the reason that SSL is easy to deploy is because it is extremely flexible and, in turn, able to support a tremendously diverse set of users, systems, and operating conditions. System developers, administrators, and vendors of SSL-enabled products can establish support for numerous encryption protocols and ciphers all at once, employ self-signed certificates, and even get by using certificates configured for one system on a completely different resource. The problem is that all of this flexibility opens the door to "mistakes," such as configurations that result in the trust-related issues discussed previously, or the use of encryption protocols, hashing algorithms, and ciphers that are regarded as weak. Another complicating factor is that although these are mistakes from a security perspective, they're actually favorable configurations from the perspective of trying to minimize costs and maximize the usability/reach of an application. As a result, they may in fact be selected/allowed on purpose by developers and administrators that are unaware of the security implications or that consider the tradeoffs acceptable.

SSL is not immune to attacks. Finding a vulnerability in a standard encryption algorithm or cipher is an extremely rare, if not unheard of event. Far less rare, however, are weaknesses introduced at the protocol (i.e., SSL/TLS) and systems/application levels by poor implementation of these cryptographic primitives. This is not unexpected. Cryptography and cryptographic systems are generally complex and poorly understood. The result, as with other complex systems, is that vulnerabilities are in fact present and, furthermore, that successful exploits are inevitable. Current examples pertaining to SSL include the BEAST and CRIME attacks, and lingering Insecure Renegotiation vulnerabilities.

SSL is used for far more than web/e-commerce traffic. When it comes to SSL, many organizations and security tools focus their attention primarily (if not exclusively) on its use with web applications and services. In reality, SSL is far more pervasive. It can be implemented for practically any type of application, and is commonly used for everything from email, file transfer, collaboration, and secure remote access solutions to the management interfaces of routers, switches, firewalls, wireless access points and servers. Moreover, it is not confined to port 443 or the handful of other well-known SSL ports. Implementations can take advantage of any random port, and some do! Organizations also need to be mindful that SSL is not used solely for inbound and intranet communications. Many internally initiated SSL sessions to external sites are benign – for example, an employee doing some online banking during their lunch break. However, outbound sessions can also involve users taking advantage of undesirable/unauthorized services, such as anonymous proxies or cloud storage utilities – or worse, entrenched bots/malware exfiltrating data or communicating with their command and control servers.

The bottom line is that far too many organizations under-estimate the extent to which SSL is employed in their computing environments, the threat of it being misused, and the degree to which their SSL implementations are potentially vulnerable. In doing so, these organizations not only run an increased risk of exposing sensitive data, but also of failing compliance audits (e.g., PCI-DSS) and actually losing business due to abandoned transactions and erosion of customer confidence and trust.

HOW TENABLE CAN HELP

Tenable's SecurityCenter platform combines in-depth vulnerability and configuration auditing with real-time network monitoring, robust event correlation, and extensive analysis capabilities to deliver unparalleled insight into an organization's SSL usage and exposure to related vulnerabilities and threats.

With the Tenable solution, enterprises not only obtain a single, role-based interface for administrators, auditors, and risk managers to evaluate, communicate, and report information necessary for effective decision making and systems management. They also benefit from a wealth of integral capabilities that help transform the false sense of security most organizations have with their SSL implementations – and with SSL usage in general – into real security. Detailed in the following sections, these capabilities include:

- Detecting security and trust issues with SSL digital certificates that have the potential to materially impact a company's bottom line
- Detecting SSL configuration issues that result in a false sense of security and might cause an organization to fail one or more of its compliance audits
- Detecting vulnerabilities in SSL implementations that could lead to successful attacks and exposure of sensitive information
- Detecting all SSL usage within an organization – instead of just the traffic associated with common SSL ports
- Detecting communications for which SSL is not enabled but probably should be; and,
- Detecting, correlating, and classifying internally-initiated SSL sessions and anomalous SSL activity to help uncover threats – such as malware infections – and minimize the unauthorized disclosure of sensitive information.

SSL VULNERABILITY, CONFIGURATION AND COMPLIANCE ASSESSMENT

Using the Tenable solution, IT departments can proactively conduct comprehensive vulnerability, configuration, and compliance assessments of SSL certificates and the systems that employ them to detect a wide range of potentially significant security and trust-related issues. Moreover, unlike competing tools that focus only on web services operating on a handful of well-known SSL ports, the Tenable solution can be configured to perform these assessments across all ports and applications. This ensures that none of an organization's SSL implementations – sanctioned or otherwise – are able to slip through the cracks.

Detecting SSL certificate and server/application configuration issues. The Tenable solution finds and examines both SSL certificates and the systems/applications that use them for numerous security and trust-oriented configuration problems. Related issues that can be uncovered include:

- Certificates with weak private keys (e.g., less than 1024 bit)[2]
- Certificates that have been signed by weak hashing algorithms (which could lead to spoofing/man-in-the-middle attacks)
- Self-signed and unsigned certificates
- Certificates from unknown/untrusted certificates authorities
- Mismatch between host/domain name and the common name on the certificate
- Certificates that are not yet valid
- Certificates that are expired or revoked
- Support for weak protocols (e.g., SSLv2)
- Support for weak cipher suites (e.g., NULL cipher)
- Support for anonymous key exchange (i.e., no authentication required)
- Invalid trust chains
- Failure to implement Strict Transport Security (a safety-net mechanism that can be used to ensure that all communications with a web site are SSL protected)
- Non-compliant/incomplete use of Strict Transport Security

Any of these conditions could be cause for session abandonment or, worse, result in an implementation that is susceptible to one or more forms of attack.

Certificate Plugins

Plugin ID	Total	Severi...	Name	Family
4803	27	Low	SSL Certificate Signed Using Weak Hashing Algorithm	Generic [PVS]
7052	4	Info	SSL cert expiration date information	Generic [PVS]
10863	12	Info	SSL Certificate Information	General
15901	2	Medium	SSL Certificate Expiry	General
21643	15	Info	SSL Cipher Suites Supported	General
35291	5	Medium	SSL Certificate Signed using Weak Hashing Algorithm	General
45410	3	Info	SSL Certificate commonName Mismatch	General
45411	2	Medium	SSL Certificate with Wrong Hostname	General
51192	12	Medium	SSL Certificate Cannot Be Trusted	General
56984	15	Info	SSL / TLS Versions Supported	General
57582	4	Medium	SSL Self-Signed Certificate	General

Figure 1: Example of Certificate Issues

Detecting SSL-related compliance issues. Reliable cryptography is often a focal point for industry standards and regulations. For example, Requirement 4 of the Payment Card Industry Data Security Standard (PCI-DSS) specifies the need to "encrypt transmission of cardholder data across open, public networks." It further details the need to:

- Use strong cryptography and security protocols such as SSL/TLS;
- Verify that only trusted keys and/or certificates are accepted; and,
- Verify that proper encryption strength is implemented for encryption methodology in use.

Using a corresponding subset of the checks discussed above, enterprise IT can easily establish, maintain, and demonstrate compliance with these and any similar requirements specified in other regulations and standards.

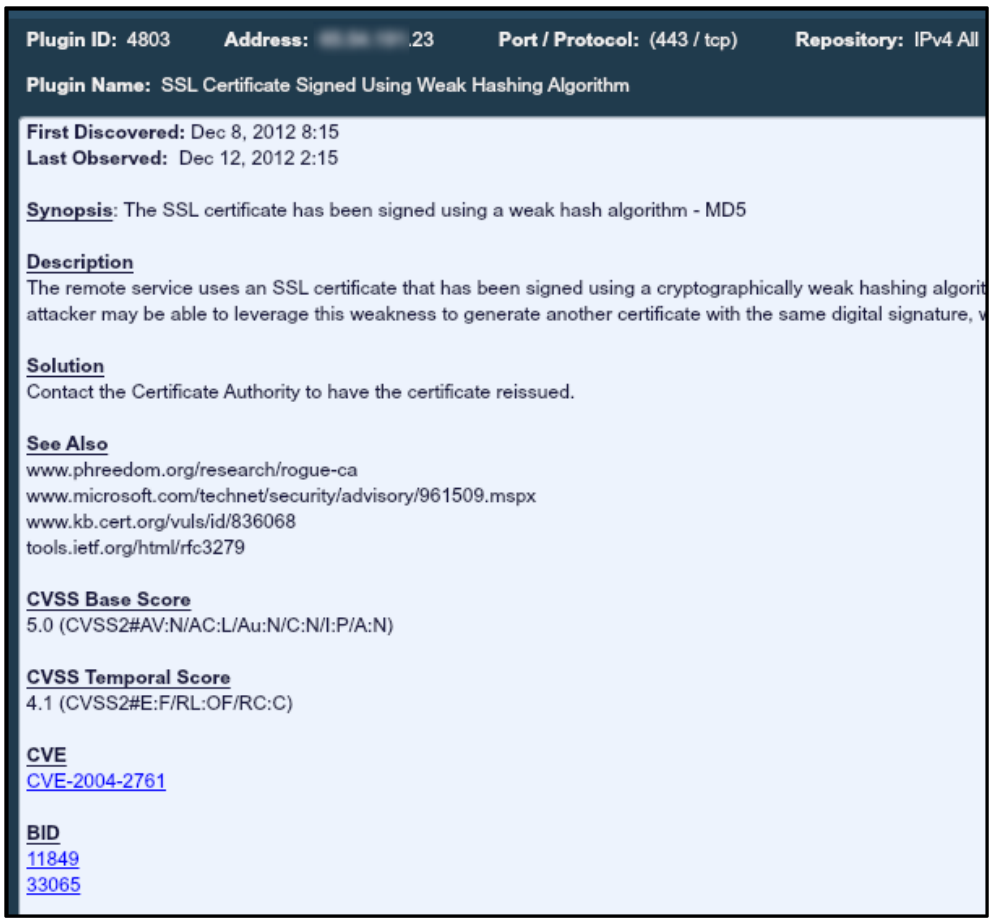
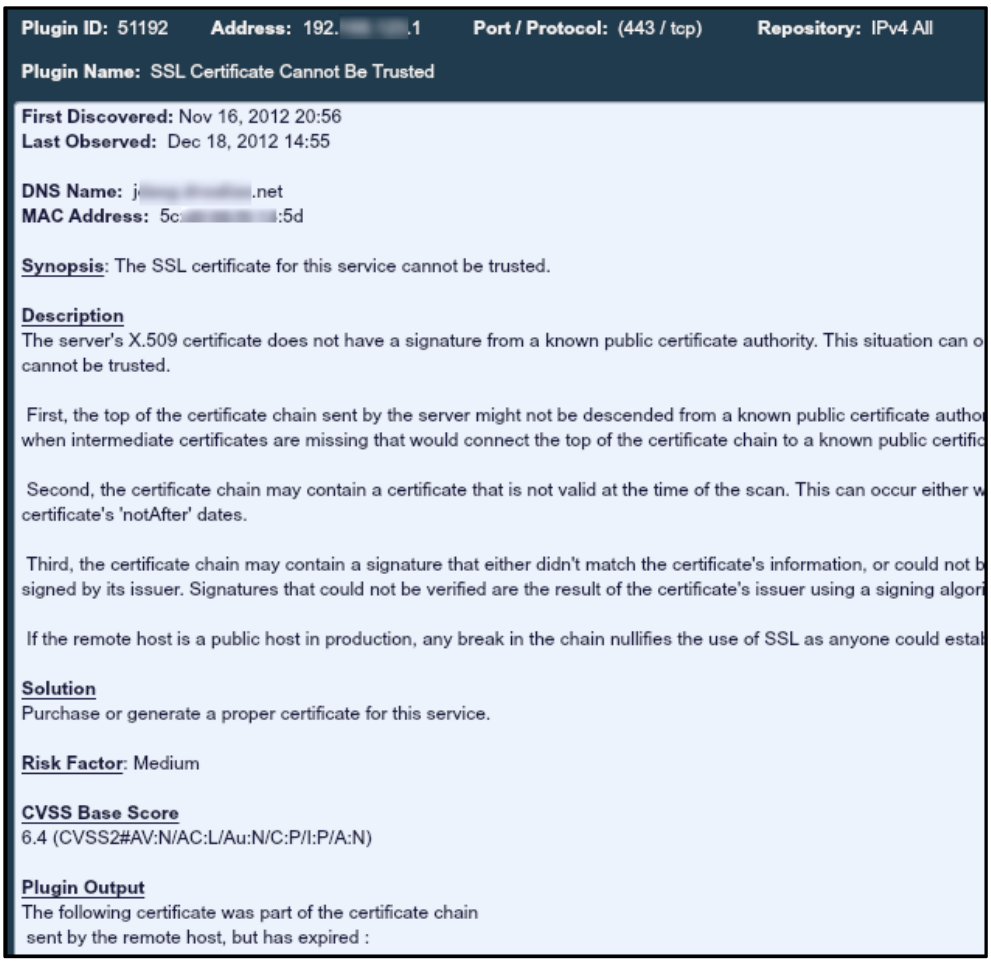


Figure 2: Example of Weak SSL Certificate Strength

Detecting other SSL vulnerabilities. As discussed, issues with SSL are not limited to certificate and server configuration "mistakes." Accordingly, the Tenable solution also includes the ability to detect both broad-spectrum and vendor-specific vulnerabilities introduced at the protocol, system, and application levels. Representative checks include those for:

- Insecure renegotiation of SSL connections
- Susceptibility to SSL renegotiation DoS attacks
- Systems susceptible to the TLS CRIME attack
- Low entropy Debian keys
- Unprotected admin interfaces on Cisco VPN concentrators
- Juniper routers with web interfaces that support weak ciphers



Plugin ID: 51192 **Address:** 192. .1 **Port / Protocol:** (443 / tcp) **Repository:** IPv4 All

Plugin Name: SSL Certificate Cannot Be Trusted

First Discovered: Nov 16, 2012 20:56
Last Observed: Dec 18, 2012 14:55

DNS Name: j .net
MAC Address: 5c :5d

Synopsis: The SSL certificate for this service cannot be trusted.

Description
The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can o
cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate author
when intermediate certificates are missing that would connect the top of the certificate chain to a known public certific

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either w
certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not b
signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algori

If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could estab

Solution
Purchase or generate a proper certificate for this service.

Risk Factor: Medium

CVSS Base Score
6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Output
The following certificate was part of the certificate chain
sent by the remote host, but has expired :

Figure 3: SSL Certificate Trust

REAL-TIME SSL MONITORING AND SITUATIONAL AWARENESS

Unlike competing products and technologies, the Tenable SecurityCenter platform is not limited to performing point-in-time assessments of an organization's SSL infrastructure. Complementing this foundational functionality is Tenable's support for real-time monitoring and detection of SSL usage and events, including many of the issues discussed above. Robust correlation and extensive analysis capabilities deliver further value, for example, by exposing anomalous SSL activity that might be indicative of entrenched malware and revealing the nature of encrypted user sessions to outbound sites.

Detecting web/non-web SSL. One of the strengths of Tenable's real-time monitoring is the ability to efficiently detect the sources of all SSL traffic – not just for web services but for all applications and across all ports. Unlike competing solutions, it can even detect scenarios where a single IP address hosts multiple SSL protected services. All of this information can then be used as the basis for conducting further, in-depth assessments. This approach avoids the need for extensive active scanning and is particularly beneficial for networks with systems that are unable to tolerate any type of performance degradation or outages.

Detecting and classifying outbound user activity. The Tenable solution's ability to decode and classify SSL enhanced web sites and services visited by client devices provides administrators with real-time insight into SSL-related user activity on the web. Alerts can be configured to indicate when and to what extent users are taking

advantage of a variety of SSL-obscured "services of interest," such as anonymous proxies, cloud data storage, and social media sites.

Detecting anomalous activity and potential threats. By correlating SSL activity with statistical anomalies detected on the network, administrators can uncover additional "events of interest" that deserve further investigation. Significant changes in terms of when, where, and how SSL is used on a network can be indicative of new, rogue services deployed by individual users or business units. It can also signal the presence of entrenched malware communicating with command and control servers or, worse, successfully exfiltrating major amounts of sensitive or proprietary information.

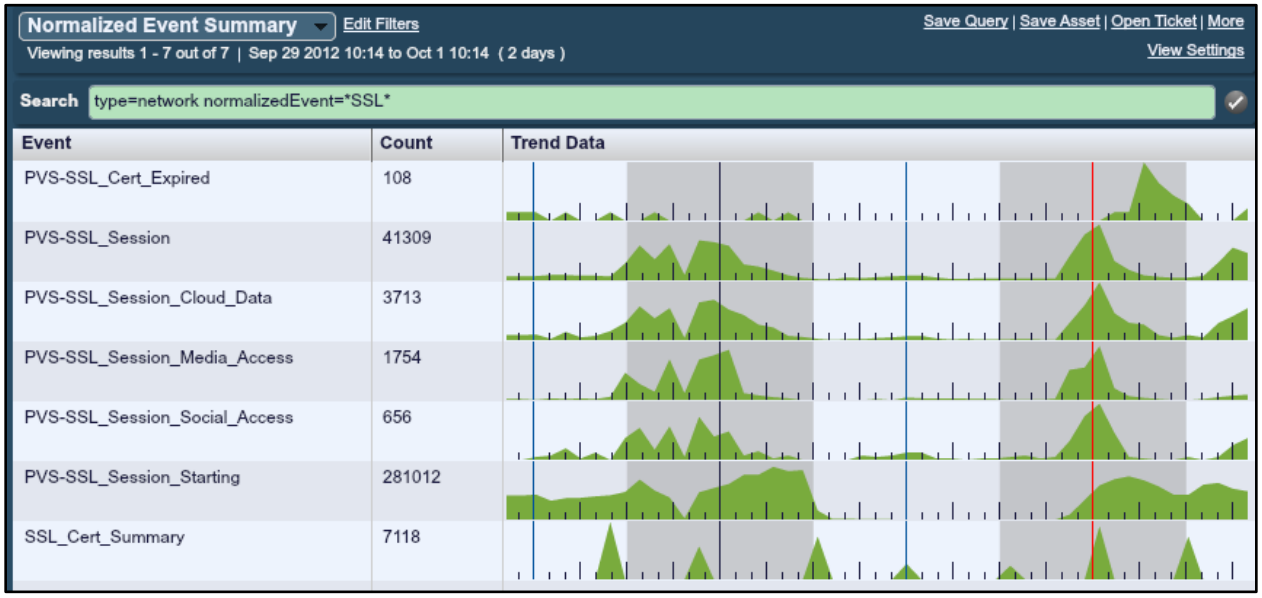


Figure 4: Anomalous SSL Event Summary

Detecting SSL omissions. Are all the communication channels that should be secured actually using SSL, or are they unprotected? That's a challenging question that administrators can now answer in a relatively straightforward manner. The Tenable solution not only detects every active web site on every web server it observes, but can also be used to record a variety of telltale events (e.g., HTTP authentications) and types of traffic (e.g., SNMP). By systematically analyzing this information, administrators can uncover unprotected web services, as well as developer, management, and other interfaces that need to be encrypted.

Providing greater situational awareness. Overall, the ability to efficiently track which systems communicate SSL, summarize SSL-based browsing activity from individual hosts over a given period of time, and correlate related events provides operations personnel with substantially greater SSL-oriented situational awareness than they would otherwise have. Associated information can subsequently be leveraged for any number of purposes, such as:

- Improving security by adjusting policies and corresponding enforcement rules;
- Enhancing the organization's posture relative to compliance with applicable standards and regulations; and,
- Narrowing the troubleshooting/forensics window and substantially reducing response times when it investigating and mitigating related incidents.

CONCLUSION – BENEFITS OF THE TENABLE SOLUTION

SSL usage is far more widespread and related security and trust issues far more common than one might expect. In this regard, enterprises that employ the SecurityCenter platform to assess and continuously monitor both their SSL infrastructure and the SSL traffic on their networks stand to gain in a number of important ways. Significant benefits include the ability to:

- Reduce operational/business risk. With the Tenable solution, administrators can easily and thoroughly detect trust-related issues with SSL certificates that may lead to erosion of customer confidence and abandoned transactions.
- Reduce security risk. Weak SSL configurations and the presence of exploitable vulnerabilities can be detected and mitigated. Unlike with competing solutions, real-time monitoring complements core assessment capabilities to provide coverage for all applications, protocols, and ports – not just those associated with web services. By providing much-needed insight into outbound SSL activity, it also helps uncover entrenched malware and unauthorized transmissions of sensitive information.
- Demonstrate compliance. Checks for the presence and strength of SSL implementations can be leveraged to establish, maintain, and demonstrate compliance with industry standards and regulations, such as the Payment Card Industry's Data Security Standard.
- Establish greater SSL-oriented situational awareness. With real-time data regarding SSL activities on the network, administrators can more efficiently and effectively troubleshoot related incidents and further ensure that the security provided by the organization's SSL infrastructure is real, and not just an illusion.

1. https://www.trustworthyinternet.org/ssl-pulse/ – Statistics provided are from the data set published October 5, 2012, and reflect assessments performed on 178,899 of the top web sites based on Alexa Traffic Rankings.

2. Some checks also have value for operational purposes. For example, consider the scenario where a software vendor indicates that its applications will no longer accept certificates with private keys shorter than 1024 bits (as was the case with Microsoft earlier this year). Given this situation, the ability of the Tenable solution to automatically check for this condition across an organization's entire computing environment delivers the added benefit of helping avoid significant degradations in terms of application functionality and network communication capabilities.

ABOUT TENABLE NETWORK SECURITY

Tenable Network Security is the de facto standard for vulnerability and compliance management solutions with over 15,000 customers worldwide. Tenable's unique real-time vulnerability and threat management technologies are used by the most demanding security professionals, compliance auditors, and executive risk managers to reduce the risk from mobile, cloud and virtual technologies. Our solutions scale to meet the needs of the smallest to the largest enterprises and government agencies including the entire U.S. Department of Defense.

For more information, please visit Tenable.com.