SECURITY INFORMATICS

Regional Centre of Excellence for Application Security, Lucknow

INSIDE THIS ISSUE

Security Informatics

A Quarterly Publication

January 2023- March 2023

Regional Centre of Excellence for Application Security, Lucknow

Under the immense leadership of

Shri R H Khan

Dy. Director General &
State Informatics Officer, NIC Uttar Pradesh

&

Under the direction of

Shailesh Kumar Srivastava

HoD, CoEAS-UP & Senior Director (IT)

Team Members

Ravikar Srivastava, *Deputy Director (IT)*

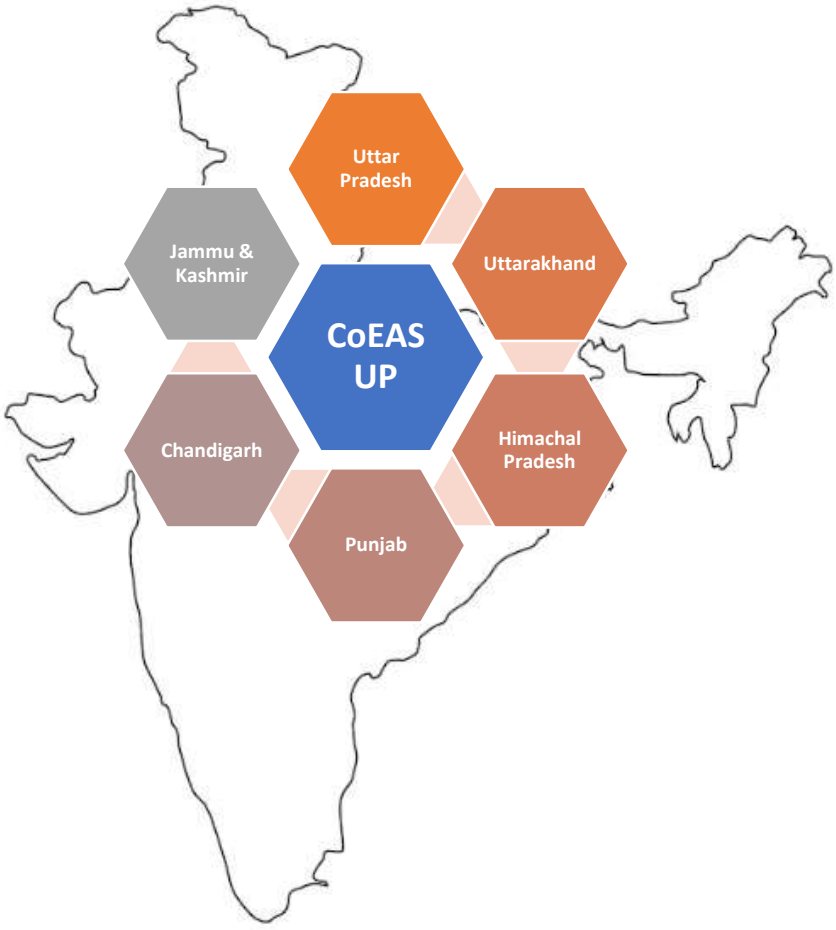
Aparna Khare, *Deputy Director (IT)*

Divyanshi Kushwaha, *Assistant Director (IT)*

Aviral Awasthi, *Assistant Director (IT)*

Introduction

As the number of web and mobile applications being developed and deployed by National Informatics Centre continues to grow with new and emerging technologies, the demand for application security audits and penetration testing has also risen in response to the increasing risks posed by cyber security threats. In addition to the increasing demand for application security audits and penetration testing, there is also a growing need for SSL and TLS compliance activities. With the rise of cyber security threats, ensuring secure data transmission and communication between servers and clients has become paramount. Complying with SSL and TLS protocols in safeguarding sensitive information and protecting against unauthorized access is vital. The Regional Centre of Excellence for Application Security at Lucknow aims to ensure the security compliance is met for the seven states under purview.



The Regional Centre of Excellence for Application Security, Lucknow handles application security activities for seven states, namely, ***Uttar Pradesh, Uttarakhand, Himachal Pradesh, Punjab, Chandigarh and Jammu & Kashmir.***

Work Highlights

Centre Of Excellence for Application Security, Lucknow Work Highlights

ACTIVITIES UNDERTAKEN

Several activities were undertaken to enhance the safety and security of web applications, including infrastructure scans (300+), penetration testing (20+ new tickets, and 50+ follow ups), black box audits and white box audits, manual audits, SSL compliance scans, and development of modules for CoEAS applications (ASTS and ASAMS). However, for this quarter, the major focus is on SSL compliance activity. The rise of cyber threats and the need for secure data transmission have made SSL compliance a critical aspect of web application security. Therefore, the organization is allocating more resources and attention towards ensuring that its web applications are compliant with SSL protocols and standards, safeguarding sensitive information and protecting against unauthorized access. The SSL compliance activity is crucial in maintaining the highest level of security for the organization's web applications and infrastructure, enabling it to stay ahead of potential security risks and threats.

DEVELOPMENT ACTIVITIES

Following applications/tools were developed by the team members of CoEAS-UP:

1. New Application Security Ticketing System (Multi module development including assignment module, reporting module and ticketing module) in Java.
2. SSL/TLS Compliance Testing and Reporting tool in Python.

SSL/TLS COMPLIANCE

The SSL/TLS Compliance activities undertaken for the states has been influential in correcting the security posture. Himachal Pradesh has the highest compliance percentage with 99% at present, followed by Uttarakhand with 96%, overall, the compliance rate for SSL security was found to be relatively high for all states, ranging from 63% to 99%.

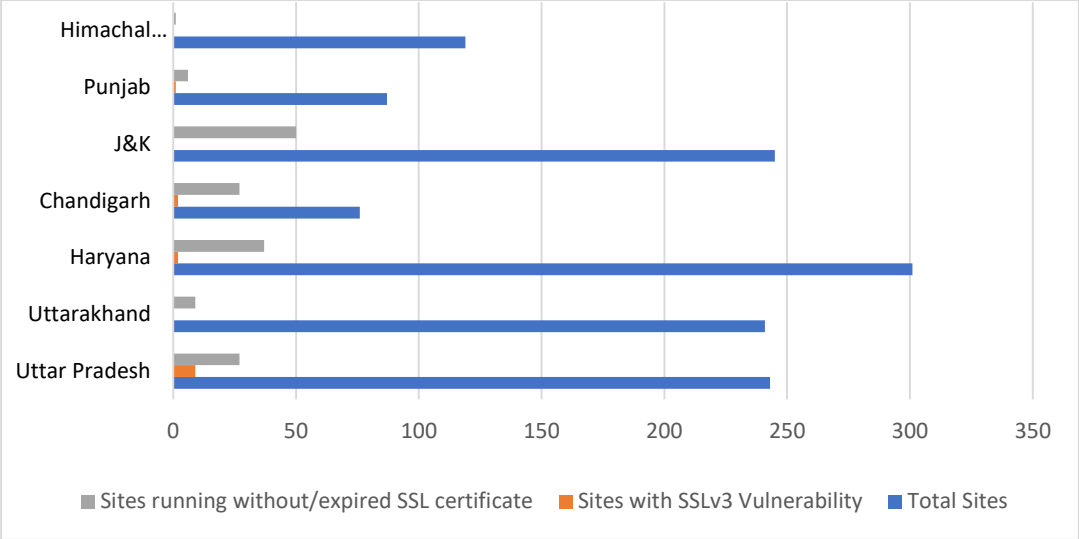


Figure 1: SSL/TLS Compliance Statistics

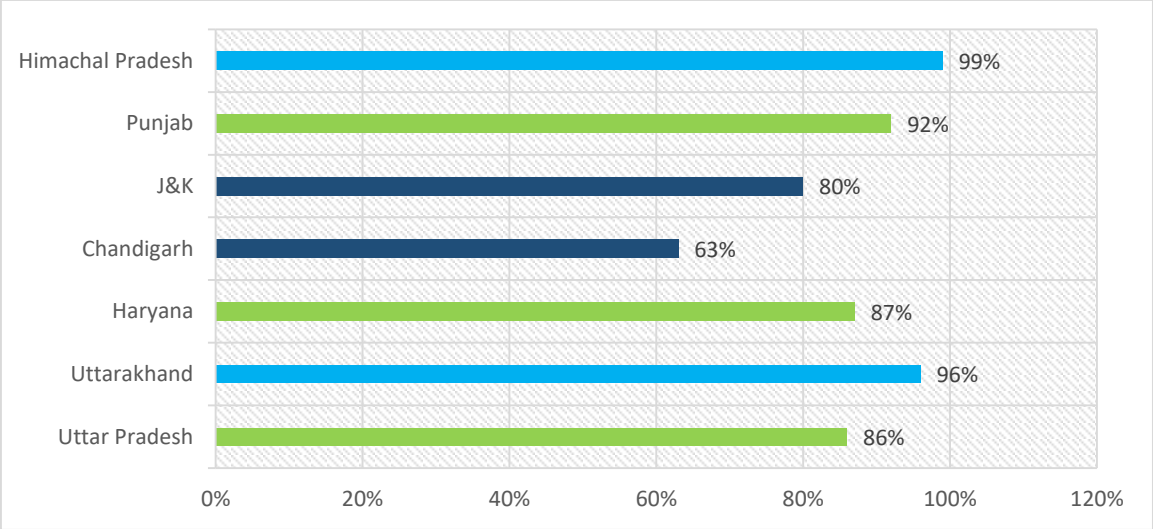
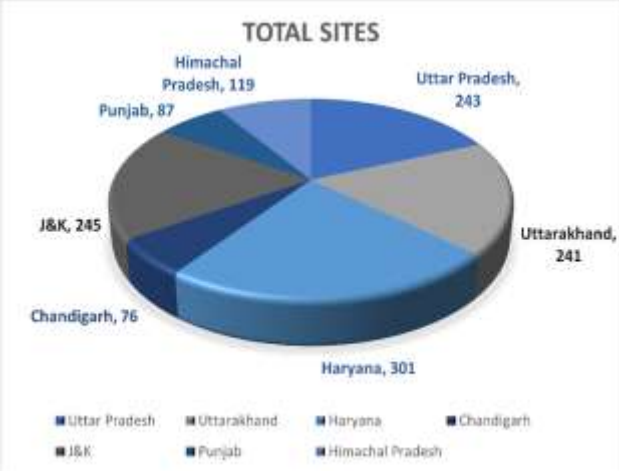
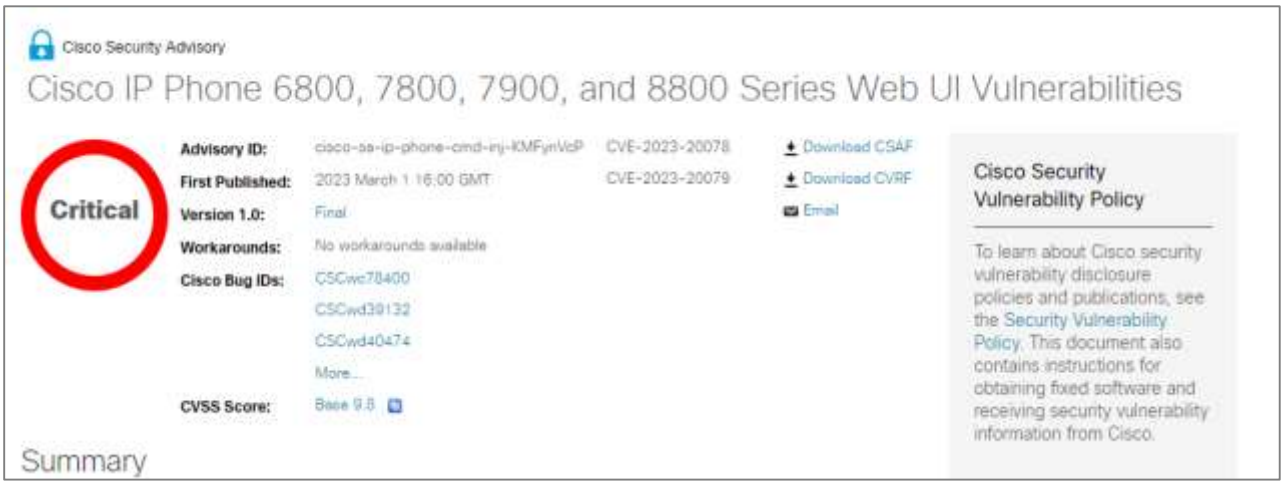


Figure 2: Compliance Percentage Comparison for the Seven States (Data as on 31st March 2023)



Recent Incidents

Critical Flaw in Cisco IP Phone Series Exposes Users to Command Injection Attack



Cisco has recently rolled out security updates to address a critical flaw impacting its IP Phone 6800, 7800, 7900, and 8800 Series products. The vulnerability, tracked as CVE-2023-20078, is rated 9.8 out of 10 on the CVSS scoring system and is described as a command injection bug in the web-based management interface arising due to insufficient validation of user-supplied input. Successful exploitation of the bug could allow an unauthenticated, remote attacker to inject arbitrary commands that are executed with the highest privileges on the underlying operating system.

"An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface," Cisco said in an alert published on March 1, 2023. CVE-2023-20079 (CVSS score: 7.5), also a result of insufficient validation of user-supplied input in the web-based management interface, could be abused by an adversary to cause a DoS condition.

While Cisco has released Cisco Multiplatform Firmware version 11.3.7SR1 to resolve CVE-2023-20078, the company said it does not plan to fix CVE-2023-20079, as both the Unified IP Conference Phone models have entered end-of-life (EoL).

The advisory comes as Aruba Networks, a subsidiary of Hewlett Packard Enterprise, released an update to ArubaOS to remediate multiple unauthenticated command injection and stack-based buffer overflow flaws (from CVE-2023-22747 through CVE-2023-22752, CVSS scores: 9.8) that could result in code execution.

Resources for Further Reading:

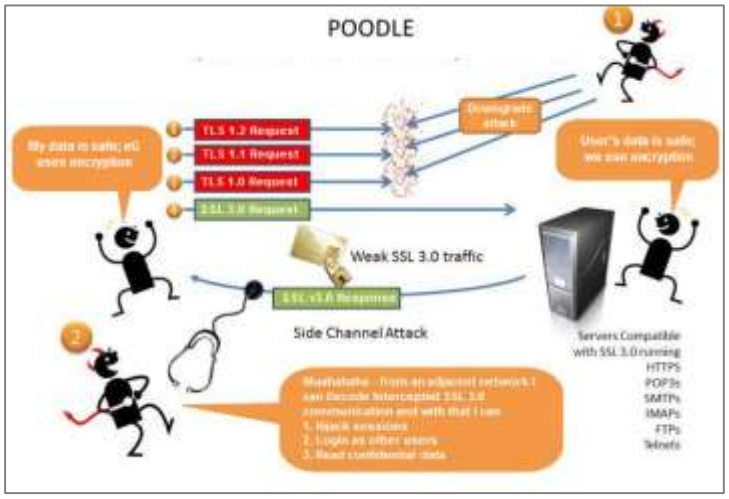
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP

Knowledge Hub

Understanding HTTPS Vulnerabilities Series 1: Poodle Attacks

WHAT IS A POODLE ATTACK?

The POODLE attack (Padding Oracle on Downgraded Legacy Encryption) exploits a vulnerability in the SSL 3.0 protocol (CVE-2014-3566). This vulnerability lets an attacker eavesdrop on communication encrypted using SSLv3. The vulnerability is no longer present in the Transport Layer Security protocol (TLS), which is the successor to SSL (Secure Socket Layer). The POODLE vulnerability lets the attacker eavesdrop on encrypted communication. This means that the attacker can steal confidential data that is transmitted, for example, passwords or session cookies, and then impersonate the user.



POODLE ATTACK.
Image Source: https://www.eginnovations.com/blog/poodle-attack-vulerability/

The attack needs to be successful in three stages:

1) In the first stage, the attacker must perform a successful man-in-the-middle attack (MITM). The attacker can now listen to all communication between the client and the server as well as add to this communication (impersonate the client or the server). However, if this is a secure connection, communication is encrypted using SSL/TLS, so the attacker cannot understand what is being sent.
2) In the second stage, the attacker must convince the server to use the old SSL 3.0 protocol. The attacker can do this by dropping connections – after a number of such drop-outs, the server will try an older protocol, thinking that the client cannot use a newer protocol such as TLS 1.2. This is called a protocol downgrade attack or downgrade dance.
3) In the third stage, when the client and the server are communicating using SSL 3.0, the attacker can use the POODLE attack to decrypt selected parts of the communication and steal confidential information.

4) To make sure that the POODLE attack succeeds, the attacker should also be able to trick the user browser into running JavaScript, for example, using social engineering.

The POODLE attack is possible due to several features of the SSL/TLS protocol. The POODLE vulnerability affects cipher suites that include symmetric encryption together with block ciphers, for example, AES or DES algorithms.

HOW THE ATTACK IS PERFORMED

To perform a typical POODLE attack and steal a web session cookie, the attacker does the following:

1) The attacker tricks the victim's browser into running JavaScript code that lets the attacker perform the attack.
2) The attacker's JavaScript code tricks the user browser into sending multiple legitimate requests to the server. These requests include the session cookie.
3) The JavaScript code modifies the connection URL (adding extra characters) so that the length of the data sent to the server is a multiple of the block size (for example, 8). This means that the last block will contain only padding (see the explanation above).
4) The attacker knows which blocks of data contain the session cookie. For example, the data may have 10 blocks and the attacker knows that the third and fourth blocks contain the session cookie value.
5) The attacker copies the entire third block to the last block and sends it to the server many times, changing something in the connection URL every time so that the MAC is different.
6) After at most 256 times, the message will be accepted. This means that the last byte of the third block, after decryption, will be the number 07, which signifies correct padding.
7) Now the attacker knows the decrypted last byte and they can combine it with previous blocks using XOR operations to obtain the real last byte of the third block.
8) The attacker can then make the connection URL one byte longer and repeat the steps above to get the next piece of the cookie. And then repeat again for the fourth block of data.
9) If the cookie length is 16, the attacker will know the cookie after no more than 4096 requests, which takes at most a few minutes.

HOW TO PROTECT AGAINST POODLE ATTACK

To protect your server against POODLE, configure it to support only TLS 1.2 and no older protocols. All older SSL and TLS versions are now officially deprecated and all modern browsers such as Chrome, Firefox, and Internet Explorer support TLS 1.2.

Resources for Further Reading:

https://www.eginnovations.com/blog/poodle-attack-vulerability

Advisories

List of Advisories

- Ensure that SSL/TLS certificates are kept up-to-date and are not expired or revoked.
- Strong and unique private keys should be used to secure SSL/TLS certificates.
- Implement TLS 1.2 or higher to ensure stronger encryption of data in transit.
- Disable SSLv2 and SSLv3 as they are known to have vulnerabilities, including the Diffie-Hellman vulnerability.
- Use HSTS (HTTP Strict Transport Security) to prevent downgrade attacks and enforce HTTPS.
- Implement secure cipher suites to ensure stronger encryption of data.
- SSL/TLS traffic should be monitored for potential security risks and anomalies.
- Web applications should be regularly scanned for SSL/TLS vulnerabilities and potential weaknesses should be identified through penetration testing.
- Educate employees and users on best practices for SSL/TLS security, such as avoiding public Wi-Fi networks and verifying SSL/TLS certificates before transmitting sensitive information.
- Stay up-to-date on the latest SSL/TLS vulnerabilities and advisories, including the Diffie-Hellman vulnerability, and apply patches and updates promptly to mitigate potential risks.

In case of any queries, may contact:

Shailesh Kumar Srivastava
Senior Director (IT)
NIC, U P State Centre
III floor, Yojana Bhawan, Lucknow-226001

email - **shailesh.srivastava@nic.in**
IP Phone- **47055**