Main Website Vulnerabilities

Team 1.5

Website: https://vtopcc.vit.ac.in/vtop/login

Host Fully Qualified Domain Name (FQDN) Resolution

Description: It was possible to resolve the name of the remote host.

Business Impact: Properly managing FQDN resolution is critical for cybersecurity. Attackers can manipulate DNS records to redirect users to malicious websites or intercept sensitive data. A strong FQDN resolution system can help protect against DNS-related attacks.

Vulnerability Path: 115.240.194.17

HTTP/2 Cleartext Detection

Description: The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

Solution: Limit incoming traffic to this port if desired.

Business Impact: Depending on the industry and location of a business, there may be legal requirements to encrypt certain types of data. Cleartext detection is essential for complying with these regulations, which can have significant legal and financial implications.

Vulnerability Path: 115.240.194.17

OS Identification

Description: Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Business Impacts: An OS identification vulnerability might reveal the specific operating system version and its associated vulnerabilities. Attackers can use this information to target known vulnerabilities in the OS, potentially gaining unauthorized access to the system. This could lead to data breaches, data loss, and damage to the organization's reputation.

Vulnerability Path: 115.240.194.17

46215 - Inconsistent Hostname and IP Address

Description: This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and leave unclosed connections on the remote target, if the network is loaded.

Solution:

Protect your target with an IP filter.

Business Impact:

Inconsistent hostname and IP address configurations can lead to network disruptions and connectivity issues. Inconsistent configurations can be exploited by malicious actors to launch attacks on your network. This can result in incorrect routing, failed DNS resolution, and other configuration-related issues that affect the functionality and reliability of your network.

Vulnerability Path:

122.187.117.185

45410 - SSL Certificate 'commonName' Mismatch

Description: The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution:

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Business Impact:

This mismatch can be exploited by attackers to launch man-in-the-middle (MITM) attacks, intercept sensitive data, or impersonate the legitimate website. This poses a significant security risk to both the business and its customers.

Vulnerability Path:

122.187.117.185

SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Description: The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm. These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service. Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

Business Impact:

Weak hashing algorithms, such as MD5 or SHA-1, are susceptible to cryptographic attacks. Attackers can exploit these vulnerabilities to forge certificates, intercept encrypted data, or impersonate a legitimate website. Search engines like Google consider website security when ranking search results. Sites with SSL certificates signed using weak algorithms may experience a decline in search engine rankings, leading to reduced online visibility and potentially decreased organic traffic. Various industry standards and regulations (e.g., PCI DSS) require websites to use strong encryption and secure hashing algorithms. Using weak hashing algorithms can lead to non-compliance, potentially resulting in fines and legal consequences.

Vulnerability Path:

122.187.117.185

Apache Tomcat Detection - Remote Code Execution

Description

Nessus was able to detect a remote Apache Tomcat web server. The installed Tomcat version is 9.0.20. The version of Tomcat installed on the remote host is prior to 9.0.35. It is, therefore, affected by a remote code execution vulnerability as referenced in the fixed_in_apache_tomcat_9.0.35_security-9 advisory. An arbitrary file read vulnerability exists in Tomcat's Apache JServ Protocol (AJP) due to an implementation defect. A remote, unauthenticated attacker could exploit this to access files which, under normal conditions, would be restricted. If the Tomcat instance supports file uploads, the vulnerability could also be leveraged to achieve remote code execution. (CVE-2020-1938)

Business Impact:

This Apache Tomcat vulnerability presents a critical business impact, including the risk of data breaches with financial, legal, and reputational repercussions, potential service disruptions causing revenue loss and customer dissatisfaction, the specter of non-compliance with data protection regulations leading to substantial fines and legal liabilities, erosion of customer trust, and reputational damage with the potential loss of competitive advantage, as well as operational and financial impacts through remediation efforts, legal costs, and resource allocation for mitigation.

Vulnerability Path: 122.187.117.185

Apache Tomcat Detection - Request Smuggling Vulnerability

Description

The version of Tomcat installed on the remote host is 9.0.0-M1 or later but prior to 9.0.68. It is, therefore, affected by a request smuggling vulnerability as referenced in the fixed_in_apache_tomcat_9.0.68_security-9 advisory. If Tomcat was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (not the default), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.

Business Impact:

In the presence of a reverse proxy that also fails to reject requests with invalid headers, this vulnerability allows for malicious actors to potentially manipulate and compromise the server's behavior, leading to potential data breaches, service disruptions, and reputational damage. The consequences include data integrity risks, loss of service availability, potential regulatory non-compliance, and the erosion of customer trust, all of which can result in financial loss and legal liabilities. Addressing this vulnerability promptly is crucial to mitigate these risks and ensure the security and resilience of your web server infrastructure.

Vulnerability Path: 122.187.117.185

Apache Tomcat Detection - Privilege Escalation Vulnerability

Description

The version of Tomcat installed on the remote host is prior to 9.0.30. It is, therefore, affected by a privilege escalation vulnerability as referenced in the 'Fixed in Apache Tomcat 9.0.30' advisory.

- When using FORM authentication there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability. (CVE-2019-17563)

Business Impact:

The privilege escalation vulnerability found in the pre-9.0.30 Apache Tomcat version introduces a significant security risk, as it opens the door to potential session fixation attacks, jeopardizing data integrity and confidentiality. While considered challenging to exploit, it presents a credible threat that could result in unauthorized access, operational disruptions, reputational damage, regulatory non-compliance, and resource allocation for mitigation, including legal liabilities, making it imperative to promptly update to a secure version (9.0.30 or later) to mitigate these potential business impacts.

Vulnerability Path: 122.187.117.185

Web Server No 404 Error Code Check

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning instead a site map, search page or authentication page.

Business Impact:

Not returning a 404 error for missing pages might provide misleading information to users. They may think that content is available when it's not, leading to frustration.

Vulnerability Path: 122.187.117.185