Comprehensive Security Assessment Report for itsecgames.com

TABLE OF CONTENTS

Vulnerabilities by Host

Exploitable Vulnerabilities Report

SSL/TLS Assessment

Mitigation Recommendations

Vulnerabilities by Host

itsecgames.com

2	4	9	2	21
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 38

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.6639	106608	OpenSSH 5.4 < 7.1p2 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0218	90022	OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security By
HIGH	7.8	5.9	0.9239	93194	OpenSSH < 7.3 Multiple Vulnerabilities
HIGH	7.5	3.6	0.2875	35450	DNS Server Spoofed Request Amplification DDoS
HIGH	7.3	6.7	0.0224	96151	OpenSSH < 7.4 Multiple Vulnerabilities
HIGH	8.5*	1.4	0.1017	84638	OpenSSH < 6.9 Multiple Vulnerabilities
MEDIUM	6.8	6.1	0.6636	159491	OpenSSH < 8.0
MEDIUM	6.5	6.1	0.6373	187201	OpenSSH < 9.6 Multiple Vulnerabilities
MEDIUM	6.4	3.8	0.5675	90023	OpenSSH < 7.2p2 X11Forwarding xauth Command Injection
MEDIUM	6.1	6.7	0.3016	85382	OpenSSH < 7.0 Multiple Vulnerabilities
MEDIUM	5.9	-	-	99359	OpenSSH < 7.5
MEDIUM	5.9	6.1	0.6373	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.3	1.4	0.0284	103781	OpenSSH < 7.6
MEDIUM	5.3	4.9	0.9217	159490	OpenSSH < 7.8
MEDIUM	5.0*	4.2	0.0132	10539	DNS Server Recursive Query Cache Poisoning Weakness
LOW	3.8	2.4	0.0001	234554	OpenSSH < 10.0 DisableForwarding
LOW	2.1*	2.2	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	11002	DNS Server Detection

INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	10919	Open Port Re-check
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Exploitable Vulnerabilities Report

Exploitable vulnerabilities create gaps in the network's integrity, which attackers can take advantage of to gain access to the network. Once inside the network, an attacker can perform malicious attacks, steal sensitive data, and cause significant damage to critical systems. This report provides a summary of the most prevalent exploitable vulnerabilities.

Exploitable Vulnerabilities: Top 25

The Exploitable Vulnerabilities: Top 25 table uses the plugin attribute "exploit_available" to identify software that has working exploits in the wild. The data is then sorted using the count, which is a representation of the affected hosts. While some plugins may be present more than one time on a single host, for the most part a plugin will only be present once on each host. This list of vulnerabilities exposes the organization to many different attach frameworks and script kiddie attacks. These vulnerabilities should be prioritized and the software removed or updated to a supported version as soon as possible.

Severity (CVSS v3.0)	Plugin ID	Plugin Name	Count
HIGH	93194	OpenSSH < 7.3 Multiple Vulnerabilities	1
HIGH	96151	OpenSSH < 7.4 Multiple Vulnerabilities	1
MEDIUM	85382	OpenSSH < 7.0 Multiple Vulnerabilities	1
MEDIUM	90023	OpenSSH < 7.2p2 X11Forwarding xauth Command Injection	1
MEDIUM	159490	OpenSSH < 7.8	1
MEDIUM	159491	OpenSSH < 8.0	1
MEDIUM	187201	OpenSSH < 9.6 Multiple Vulnerabilities	1
MEDIUM	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	1

Exploitable Vulnerabilities: Hosts by Plugin

The Exploitable Vulnerabilities: Hosts by Plugin table provides the IT operations team with an action plan and the identified hosts for each vulnerability. IT managers are able to use this information in planning patch deployments and in working with the information security team in risk mitigation efforts. The table also uses the plugin attribute "exploit_available" to identify exploitable software and then sorts the scan results using severity, then plugin ID. The entries in the "Hosts" column are then sorted in ascending order.

Severity (CVSS v3.0)	Plugin ID	Plugin Name	Hosts
HIGH	93194	OpenSSH < 7.3 Multiple Vulnerabilities	itsecgames.com
HIGH	96151	OpenSSH < 7.4 Multiple Vulnerabilities	itsecgames.com
MEDIUM	85382	OpenSSH < 7.0 Multiple Vulnerabilities	itsecgames.com
MEDIUM	90023	OpenSSH < 7.2p2 X11Forwarding xauth Command Injection	itsecgames.com
MEDIUM	159490	OpenSSH < 7.8	itsecgames.com
MEDIUM	159491	. OpenSSH < 8.0	itsecgames.com
MEDIUM	187201	OpenSSH < 9.6 Multiple Vulnerabilities	itsecgames.com
MEDIUM	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	itsecgames.com

SSL/TLS Assessment

An SSL Labs scan of **www.itsecgames.com** revealed a **certificate name mismatch**. The certificate presented by the server does not include the domain name **www.itsecgames.com**. This means browsers will warn users with “connection not private” errors, and it exposes the site to **man-in-the-middle (MITM) attacks** since the identity of the server cannot be properly verified.

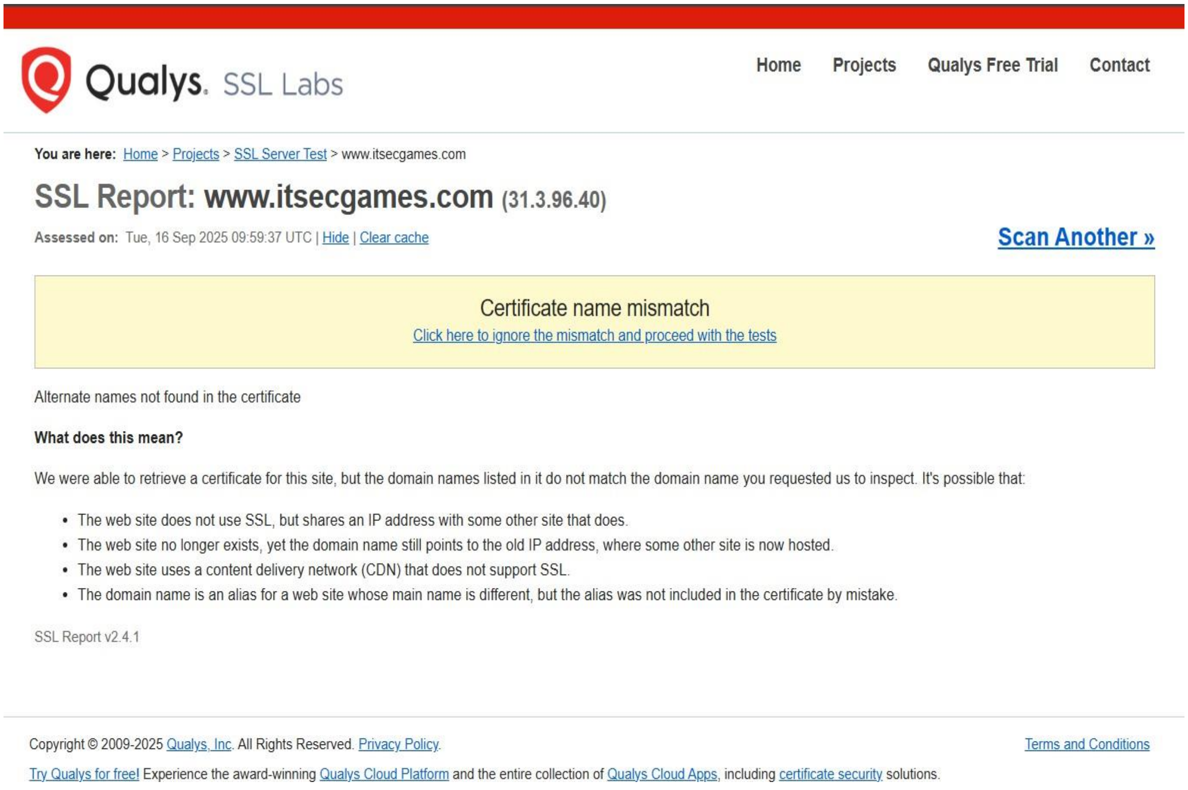
Impact:

- Users cannot reliably confirm they are connecting to the legitimate site.
- Potential for interception or spoofing of traffic.

Mitigation Recommendations:

- Obtain and install a valid SSL/TLS certificate for **www.itsecgames.com** issued by a trusted Certificate Authority (e.g., Let’s Encrypt).
- Ensure the web server is configured to serve the correct certificate for this domain.
- Enforce HTTPS-only access once the certificate is corrected.
- Additionally, disable deprecated protocols (SSLv2/SSLv3, TLS 1.0/1.1) and weak ciphers (e.g., RC4, 3DES).
- Configure the server to support only TLS 1.2/1.3 with strong cipher suites (AES-GCM, CHACHA20) and enable Perfect Forward Secrecy (ECDHE).

SSL Labs Scan Screenshot:



You are here: Home > Projects > SSL Server Test > www.itsecgames.com

SSL Report: www.itsecgames.com (31.3.96.40)

Assessed on: Tue, 16 Sep 2025 09:59:37 UTC | Hide | Clear cache

Scan Another »

Certificate name mismatch

Click here to ignore the mismatch and proceed with the tests

Alternate names not found in the certificate

What does this mean?

We were able to retrieve a certificate for this site, but the domain names listed in it do not match the domain name you requested us to inspect. It's possible that:

- The web site does not use SSL, but shares an IP address with some other site that does.
- The web site no longer exists, yet the domain name still points to the old IP address, where some other site is now hosted.
- The web site uses a content delivery network (CDN) that does not support SSL.
- The domain name is an alias for a web site whose main name is different, but the alias was not included in the certificate by mistake.

SSL Report v2.4.1

Copyright © 2009-2025 Qualys, Inc. All Rights Reserved. Privacy Policy.

Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.

Mitigation Recommendations

Critical & High Severity Issues

OpenSSH Outdated Versions (Multiple Vulnerabilities – CVSS up to 9.8)

Fix: Upgrade OpenSSH to the latest stable version (□ 9.6).

Why: Removes multiple known remote code execution and privilege escalation vulnerabilities. Reference: OpenSSH Release Notes

DNS Server Spoofed Request Amplification (DDoS risk)

Fix: Disable DNS recursion for external queries. Configure rate limiting on the DNS server. Why: Prevents amplification-based distributed denial-of-service attacks.

Medium Severity Issues

X11 Forwarding Command Injection (OpenSSH < 7.2p2)

Fix: Disable X11 forwarding unless absolutely required. Upgrade SSH server to a patched version. Why: Prevents remote attackers from injecting malicious commands.

Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Fix: Apply vendor patches that disable affected SSH key exchange methods. Why: Mitigates man-in-the-middle attacks on SSH connections.

Low Severity & Informational Findings

ICMP Timestamp Request Disclosure

Fix: Disable ICMP timestamp responses.

Why: Prevents attackers from determining system uptime and aiding fingerprinting.

Server and Service Information Disclosure (headers, banners, OS fingerprints)

Fix: Hide or minimize HTTP server version in response headers.

Restrict unnecessary SSH algorithms and disable weak crypto (e.g., SHA-1 HMAC). Why: Reduces exposed attack surface by limiting information available to attackers.

SSL/TLS (Gap in Current Report)

SSL/TLS Scan and Remediation

Perform a dedicated SSL/TLS scan (e.g., using Qualys SSL Labs or testssl.sh) to check:

- Certificate validity & expiration.
- Protocol support (disable SSLv2/SSLv3, weak TLS versions).
- Cipher strength (disable weak ciphers such as RC4, 3DES).

Fix: Reconfigure the web server to use only TLS 1.2/1.3 with strong cipher suites. Why: Protects data confidentiality and prevents downgrade/weak cipher attacks.

Prioritization Guidance

Immediate Action (within 7 days)

Patch OpenSSH critical vulnerabilities, disable DNS recursion, apply CVE-2023-48795 fix.

Short Term (within 30 days)

Upgrade or reconfigure SSH and DNS services, disable ICMP timestamp, restrict exposed banners.

Ongoing

Schedule regular vulnerability scans and SSL/TLS assessments to ensure continuous security posture improvement.