

Renewed SSL Certificates Are Still Taking Sites Down, SSL Dragon Warns

Weekly certificate outages hit 45% of organizations in 2025, up from 12% in 2022. SSL Dragon's free SSL Checker reports what a website really serves.

SAN JOSE, CA, UNITED STATES, July 21, 2026 /EINPresswire.com/ -- Seventy-two percent of organizations experienced at least one certificate-related outage within a twelve-month period, according to CyberArk's 2025 State of Machine Identity Security Report, a survey of 1,200 security

leaders. The same survey found 45% facing weekly outages, up from 12% in 2022. SSL Dragon, a San Jose-based provider of SSL certificates and digital security solutions, argues the problem is no longer renewal itself. Automation is renewing certificates. It is not proving they arrived.

“

Automation reports what it issued. Your server reports what visitors actually receive. Outages live in the gap between those two answers.”

Roman Munteanu, SSL Dragon

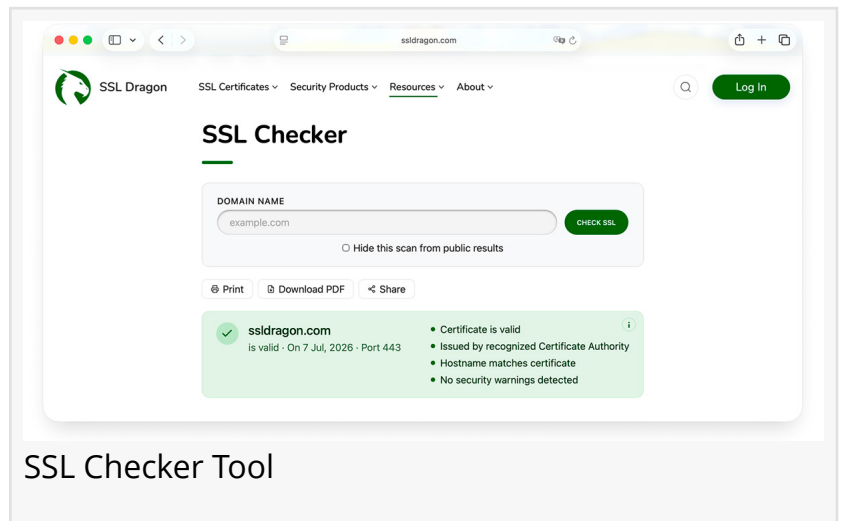
Renewal software reports what it did. A certificate was requested and issued. It does not report what a visitor's browser receives. Those are different questions, and most teams track only the first. When the answers diverge, visitors get a full-page security warning and leave.

The failures are quiet. A certificate renews, but the web server is never restarted, so it keeps serving the expiring one. A certificate installs incompletely, so it works in the administrator's browser but fails for mobile visitors. A load balancer keeps presenting an old certificate while the

server behind it holds the new one. In each case, the renewal log records success.

SSL Dragon has [documented this class of failure previously](#), noting that shorter lifespans relocate risk from forgotten renewals to broken automation rather than removing it.

The 200-day validity cap in force since March 15, 2026, leaves less margin, and it falls to 100 days



SSL Checker Tool

in March 2027 and 47 days in March 2029. Each renewal is a chance for something to break, and shorter cycles produce more of them with less time to catch a failure before visitors do.

SSL Dragon's [SSL Checker](#) answers the question a renewal log cannot. The free tool asks a public site the same thing a visitor's browser asks, then reports what came back. The certificate it finds live, and the real date on it, expose a renewal that never reached production. Whether the server hands over everything needed to trust that certificate separates a site that works at an administrator's desk from one that fails on a phone.

"Automation reports what it issued. Your server reports what visitors actually receive," said Roman Munteanu, CEO and Founder of SSL Dragon. "Outages live in the gap between those two answers. A renewal log is a record of intent, not evidence of delivery. The only report that counts is the one a visitor's browser gets."

Automated renewal through the ACME protocol handles the frequency the caps demand, but automation does not check its own work. SSL Dragon advises verifying from outside after every renewal rather than on a fixed schedule.

About SSL Dragon:

SSL Dragon is a US-headquartered web security provider dedicated to making digital trust accessible. As a platinum partner of Sectigo and DigiCert, SSL Dragon serves over 13,000 clients globally, providing streamlined SSL management, malware protection, and enterprise PKI solutions. For more information, visit www.ssldragon.com.

Roman Munteanu

SSL Dragon

+1 669-273-6227

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/927976544>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.