Searchlight Cyber Discloses Critical Remote Commnad Execution Vulnerabulity in ETQ Reliance

Vulnerabilities in the popular quality management software could expose highly sensitive data

BRISBANE, AUSTRALIA, July 22, 2025 /EINPresswire.com/
--
The Assetnote Security Research Team at Searchlight Cyber has uncovered a series of vulnerabilities in the quality management platform ETQ Reliance.

In particular, the ability to access an internal “SYSTEM” account and escalate through a Remote Code Execution (RCE) vulnerability could allow an attacker to expose the stored data, which - by the nature of the application - is likely to be sensitive. All vulnerabilities were responsibly disclosed and have been patched by ETQ Reliance.

ETQ Reliance is a system for centralized document and forms management. Despite being fairly popular, it has not received much attention from security researchers - no CVEs had been registered to the product prior to the publication of this research. Searchlight’s security researchers investigated the software because of the potential risk inherent in thousands of documents being exposed to the internet.

In total, four CVEs were disclosed, with the technical information on how the vulnerabilities were discovered detailed in the Assetnote Security Research Center:

- CVE-2025-34140 - An authentication bypass vulnerability, where requests containing the suffix `;localized-text` are allowed unauthenticated access to sensitive endpoints.
- CVE-2025-34141 - A stored cross-site scripting (XSS) vulnerability in the `SQLConverterServlet`.
- CVE-2025-34142 - A XML External Entity (XXE) injection vulnerability via the /resources/sessions/sso endpoint.
- CVE-2025-34143 - An authentication bypass vulnerability that allows login as the privileged SYSTEM user by appending a space character to the username field. This leads to remote

command execution after bypassing authentication.

The last of these is a relatively straightforward bypass in the login screen, which allowed the researchers to access an internal “SYSTEM” account. This vulnerability could be escalated to Remote Code Execution, meaning any unauthenticated attacker can completely take over an ETQ Reliance instance, including leaking all data.

Shubham Shah, SVP of Research and Engineering at Searchlight Cyber commented: “Some vulnerabilities are simpler than others. A complex exploit is not always required to compromise software. By typing a single space in ETQ Reliance's login screen, we achieved full access to the SYSTEM account, which could quite easily be escalated to remote code execution. These vulnerabilities had the potential to lead to data leaks of sensitive material.”

Searchlight Cyber’s security research team continues to perform novel zero-day and N-day security research to ensure maximum coverage and care for its customers’ attack surfaces. All research is integrated into its Attack Surface Management platform, Assetnote, which continuously monitors, detects, and proves the exploitability of exposures before threat actors can use them.

About Searchlight Cyber:

Searchlight Cyber was founded in 2017 with a mission to stop threat actors from acting with impunity. Its External Cyber Risk Management Platform helps organizations to identify and protect themselves from emerging cybercriminal threats with Attack Surface Management and Threat Intelligence tools designed to separate the signal from the noise. It is used by some of the world’s largest enterprises, government and law enforcement agencies, and the Managed Security Service Providers at the forefront of protecting customers from external threats. Find out more at www.slcyber.io.

Sonia Awan
Outbloom Public Relations
soniaawan@outbloompr.net
Visit us on social media:
LinkedIn

in today's world. Please see our Editorial Guidelines for more information.