Analysis of CVE-2025-52635

[My First M Last]

[My School]

[My CS Class]

[My Professor]

October 26, 2025

Abstract

HCL AION 2.0 suffered from a vulnerability CVE-2025-52635 that created opportunities for cross site scripting because of its insufficient enforcement by the content security policy. This issue enabled attackers to inject malicious scripts that execute in users' browsers, potentially causing data exposure or compromising systems. The vulnerability was rated by both NIST and HCL with varying degrees of criticality, NIST indicating a severe vulnerability and HCL opposing it as being a minor issue. The exploitation itself requires no privileges, no user interaction, but is restricted to the vulnerable environment. This analysis will compile details on this specific vulnerability, its implications, and significant consequences faced by companies with similar vulnerabilities.

CVE-2025-52635

A CVE (Common Vulnerabilities and Exposures) record is a public record that provides a short description of a cybersecurity failure. These can include things like the Log4j vulnerability that allowed malicious actors to execute code remotely, an example that highlights the importance of security with real consequences. CVEs are quantified by their vulnerability severity, from 0.0 to 10.0, using the metrics: attack vector, attack complexity, privileges required, user interaction, scope, and effect on confidentiality, integrity, and availability. CVE-2025-52635 is rated very differently by both NIST (National Institute of Standards and Technology) and CNA (CVE Numbering Authority), having scores of 9.8 (critical) and 3.7 (low), respectively. An important thing to note is that while a private company may have more information on its own security vulnerabilities, it may want to downplay issues in favor of its users' trust. Thus, it is important to this analysis to cover both the NIST and HCL evaluations of the CVE and other similar issues for breadth of coverage and neutrality.

CVE Details

Attack Vector

Both NIST and CNA classify this as a network-based attack vector, enabling an attacker to exploit the vulnerability over the internet, opening the vulnerability to potential attackers all across the world, as opposed to attackers within the system's network.

Attack Complexity

NIST's evaluation of the attack complexity being low contributes to its high score, whereas CNA's evaluation of the complexity being high keeps its score low. A high complexity may mean an attacker needs an advanced skillset to successfully exploit the software, whereas a low complexity may mean any person can easily exploit it.

Privileges Required

NIST and CNA once again show agreement that no privileges are required, which is dangerous for the affected software, regardless of the complexity, because any person with no permission or privilege can successfully exploit it, making this a dangerous vulnerability.

User Interaction

Exploiting the software does not require user interaction from the host to be exploited, meaning no social engineering from the attacker needs to be done, and the exploit can be done remotely and automatically.

Scope

The unchanged scope of the vulnerability relegates a potential attack to only the vulnerable environment, meaning an attacker cannot gain access to another system or attack another system through the vulnerability.

Confidentiality

The NSIT rating of the effect on the confidentiality of data within this vulnerability is high, meaning sensitive data can be stolen by an attacker. However, CNA indicates the effect on confidentiality is none, which would mean there is no danger to sensitive information.

Integrity

NIST again rates the effect of the integrity of data as high, and CNA as low. The effect an attacker can have on the integrity of the data, as indicated by NIST, may mean that an attacker can manipulate the data or edit it.

Availability

According to NIST, the effect on the availability of data is high, and to CNA is none. The effect on availability may prevent authorized users from accessing data or other system functions.

Event Analysis

A group of hackers called Magecart was able to exploit an XSS vulnerability in many online shopping sites, one of the biggest being British Airways. This vulnerability exposed hundreds of thousands of transactions with British Airways alone, exposing credit card and other user information. The catastrophic failure of security resulted in loss of revenue, lawsuits, and loss of trust in the companies affected.

Correlation

Since the posting of this CVE, the issue has been resolved without significant event, and the company HCLSoftware has introduced a migration path to a newer, more secure version. While HCLSoftware was able to patch the issue in time, many companies, along with British Airways, have felt the severe consequences of this type of vulnerability.

Conclusion

This analysis of CVE-2025-52635 shows how small, seemingly unimportant security weaknesses can have extreme consequences. Even though HCLSoftware corrected the issue with no consequences of their own by releasing an updated secure version and helping users migrate to it, the vulnerability could have led to much larger effects and consequences similar to British Airways. The importance of proper and meticulous security should not be lost in issues resolved so easily as in this case. Monitoring CVEs relating to a company’s software is an effective way of staying on top of current issues, allowing security teams to fix upcoming vulnerabilities before attackers are able to target unsafe software. In addition, companies should conduct their own testing and dedicate teams to continuously attack and attempt to break into software faster than a malicious actor is able to.

References

National Institute of Standards and Technology. (2025, October 10). CVE-2025-52635 Detail. National Vulnerability Database. Retrieved October 26, 2025, from https://nvd.nist.gov/vuln/detail/CVE-2025-52635

HCLSoftware. (2025, October 9). KB0124444 - Security Bulletin. Retrieved October 26, 2025, from https://support.hcl-software.com/csm?id=kb_article&sysparm_article=KB0124444

Thales. (2025). Magecart. Imperva. Retrieved October 26, 2025, from https://www.imperva.com/learn/application-security/magecart/

Newman, L. H. (2018, September 11). How hackers slipped by British Airways' data defenses. WIRED. https://www.wired.com/story/british-airways-hack-details/