KB0130569 - Security Bulletin

Send feedback

# Security Bulletin: Multiple security vulnerabilities affect DFXAnalytics

published 44m ago • 9 Views •

## Summary

DFXAnalytics is affected by multiple security vulnerabilities.

## Vulnerability Details

**CVE-ID**: CVE-2025-31970
**Description**: HCL DFXAnalytics is affected by an Insecure Security Header configuration vulnerability where the Content-Security-Policy does not define strict directives for object-src and base-uri, which could allow an attacker to exploit injection vectors such as Cross-Site Scripting (XSS).
**CVSS Base Score**: 5.3
**CVSS Vector**: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

**CVE-ID**: CVE-2025-59851
**Description**: HCL DFXAnalytics is affected by a Using Components with Known Vulnerabilities flaw where the application utilizes unpatched libraries or sub-components, which could allow an attacker to identify and exploit publicly known security vulnerabilities to gain unauthorized access or compromise the application.
**CVSS Base Score**: 3.7
**CVSS Vector**: CVSS:3.1/ AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

**CVE-ID**: CVE-2025-59852
**Description**: HCL DFXAnalytics is affected by an Insufficient Transport Layer Protection vulnerability where data is transmitted over the network without encryption, which could allow an attacker to compromise the confidentiality, integrity, and authentication of sensitive information.
**CVSS Base Score**: 3.7
**CVSS Vector**: CVSS:3.1/ AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

**CVE-ID**: CVE-2025-59853
**Description**: HCL DFXAnalytics is affected by an Improper Error Handling vulnerability where the application exposes detailed stack traces in responses, which could allow an attacker to gain insights into the application's internal structure, code logic, and environment configurations.
**CVSS Base Score**: 3.1
**CVSS Vector**: CVSS:3.1/ AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N

**CVE-ID**: CVE-2025-59854
**Description**: HCL DFXAnalytics is affected by an Insecure Security Header Configuration vulnerability where the application utilizes the outdated X-XSS-Protection header, which could allow an attacker to exploit browser-specific rendering flaws or bypass security controls that should instead be managed by a robust Content Security Policy (CSP).
**CVSS Base Score**: 3.1
**CVSS Vector**: CVSS:3.1/ AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N



# Affected products and versions

HCL DFXAnalytics v3.1 and below

# Remediation/fixes

Upgrade to the latest version DFXAnalytics Version 4.1

# References

Complete CVSS v3 Guide On-line Calculator v3
Complete CVSS v2 Guide On-line Calculator v2

# Related Information

HCL PSIRT blog
HCLSoftware PSIRT site
HCLSoftware Support community

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing

the links in the Reference section of this Security Bulletin.

## Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response. "HCL PROVIDES THE CVSS SCORES" "AS IS" "WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY."

Copy Permalink

### Also in 'Other Products'

Security Bulletin: Multiple security vulnerabilities affect HCL Aftermarket DPC

Security Bulletin: HCL Glovius Cloud is susceptible to a Cross-Site Request Forgery (CSRF) vulnerability (CVE-2025-62346)

Security Bulletin: HCL Glovius Cloud is susceptible to an Outdated Hash Algorithm vulnerability (CVE-2024-23589)

Security Bulletin: HCL DFMPro for 3DExp is susceptible to a Denial of Service (CVE-2007-0842)

Security Bulletin: HCL Hive Telco Observability is affected by multiple vulnerability (CVE-2023-28155, CVE-2025-54798)

View all 9 articles