hirt-sec-2020-601 : Multiple Vulnerabilities in Pentaho

Last Update: October 22, 2020

1. Overview

Multiple vulnerabilities have been found in Pentaho.

CVE-2020-24664: Reflected Cross-Site Scripting
The dashboard Editor in Pentaho through 7.x - 8.x contains a reflected Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'pho:title' attribute of 'dashboardXml' parameter.

CVSS:2.0 AV:N/AC:L/Au:S/C:P/I:P/A:N
CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVE-2020-24670: Reflected Cross-Site Scripting
The Dashboard Editor in Pentaho through 7.x - 8.x contains a reflected Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'type' attribute of 'dashboardXml' parameter.

CVSS:2.0 AV:N/AC:L/Au:S/C:P/I:P/A:N
CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVE-2020-24665: Denial of Service by XML Entity Expansion injection
The Dashboard Editor in Pentaho through 7.x - 8.x contains an XML Entity Expansion injection vulnerability, which allows an authenticated remote users to trigger a denial of service (DoS) condition. Specifically, the vulnerability lies in the 'dashboardXml' parameter.

CVSS:2.0 AV:N/AC:L/Au:S/C:N/I:N/A:P
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CWE-400: Resource Exhaustion

CVE-2020-24669: DOM Based Cross-Site Scripting
The New Analysis Report in Pentaho through 7.x - 8.x contains a DOM-based Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'Analysis Report Description' field in 'About this Report' section.

CVSS:2.0 AV:N/AC:M/Au:S/C:P/I:P/A:N
CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:N
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVE-2020-24666: Stored Cross Site Scripting
The Analysis Report in Pentaho through 7.x - 8.x contains a stored Cross-site scripting vulnerability, which allows an authenticated remote users to execute arbitrary JavaScript code. Specifically, the vulnerability lies in the 'Display Name' parameter.

CVSS:2.0 AV:N/AC:L/Au:S/C:P/I:P/A:N
CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

2. Affected Systems

+ cpe:2.3:a:hitachi:pentaho:7.0 - cpe:2.3:a:hitachi:pentaho:8.3

Security Information

Related Links

Hitachi Security Advisories
Hitachi Vulnerability Disclosure Process
Acknowledgments

3. Impact

This vulnerability allows an authenticated remote users to execute arbitrary code or to trigger a denial of service (DoS) condition.

4. Solution

Users and administrators are encouraged to upgrade to fixed version.

Data Management and Analytics
https://www.hitachivantara.com/en-us/products/data-management-analytics.html

CVE-2020-24664: Reflected Cross-Site Scripting

Remediated in >= 7.1.0.25
Remediated in >= 8.2.0.6
Remediated in >= 8.3.0.0 GA

CVE-2020-24670: Reflected Cross-Site Scripting

Remediated in >= 7.1.0.25
Remediated in >= 8.2.0.6
Remediated in >= 8.3.0.0 GA

CVE-2020-24665: Denial of Service by XML Entity Expansion injection

Remediated in >= 7.1.0.25
Remediated in >= 8.2.0.6
Remediated in >= 8.3.0.0 GA

CVE-2020-24669: DOM Based Cross-Site Scripting

Remediated in >= 8.3.0.9
Remediated in >= 9.0.0.1
Remediated in >= 9.1.0.0 GA

CVE-2020-24666: Stored Cross Site Scripting

TBD

5. References

5.1 Vulnerability Enumeration

CVE-2020-24664
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24664

CVE-2020-24665
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24665

CVE-2020-24666
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24666

CVE-2020-24669
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24669

CVE-2020-24670
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24670

5.2 Credit

HIRT thanks the following for working with us to help vulnerability handling: Andrej Šimko (CVE-2020-24664, CVE-2020-24670 and CVE-2020-24665), Klára Szvitková (CVE-2020-24669) and Stanislav Dusek (CVE-2020-24666) of Accenture.

6. Update history

2020/11/x • This webpage was newly created and published.

Masato Terada (HIRT), Naoko Ohnishi (HIRT) and Sherif Fares (Hitachi Vantara)

page top