❓ Create product case icon
The create product icon is no longer visible when you are not logged in. Use the login link in the top right hand corner to authenticate and then the icon will become visible.

✕

Rate this article
★ ★ ★ ★ ★

KB0085947 - Security Bulletin   Send feedback

Security Bulletin: HCL Domino is susceptible to a Denial of Service (DoS) vulnerability (CVE-2020-14273)

🗓 updated 2y ago • 👁 244 Views • ★ ★ ★ ★ ★

Summary

HCL Domino is susceptible to a Denial of Service (DoS) vulnerability due to insufficient input validation. An attacker could use this vulnerability to crash the server.

Vulnerability Details

CVE-ID: CVE-2020-14273
Description: HCL Domino is susceptible to a Denial of Service (DoS) vulnerability due to insufficient validation of input to its public API. An unauthenticated attacker could could exploit this vulnerability to crash the Domino server.
CVSS Base Score: 5.3 (Medium)
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Affected products and versions

HCL Domino versions 10 and 11 are affected.

Remediation/fixes

Fixes are available in HCL Domino versions 10.0.1 FP6 and 11.0.1 FP2 and later.

To download the latest Notes and Domino fixpack releases go to this location and choose the applicable product/release:

https://hclsoftware.flexnetoperations.com/flexnet/operationsportal/downloadPackageVersions.action?datatype=new&lineId=Collaboration

If you have trouble accessing the link above, please follow the instructions for using the FlexNet Portal here:
https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0073344

This vulnerability is being tracked by SPR # MOBNBQPGDF.

Workarounds and Mitigations

None.

References

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

Related Information

HCL PSIRT blog
HCL Software PSIRT site
HCL Software 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 'Domino'

System Requirements for HCL Domino
👁 7514 Views

Interim Fixes for 12.0.1x versions of HCL Notes/Domino
👁 7295 Views

HCL Notes and Domino 12.0.1 Release Notes
👁 6370 Views

Security Bulletin: Multiple Log4J / Log4Shell Security Advisory for Notes, Domino, Verse, Traveler and related products
👁 5772 Views

HCL Domino 12.0 System Requirements
👁 5015 Views

View all 695 articles