



CVE-2022-44753

Published on: Not Yet Published

Last Modified on: 03/01/2023 03:58:00 PM UTC

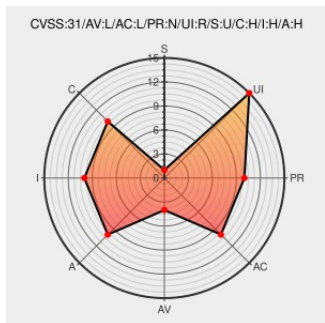
CVE-2022-44753

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Notes](#) from [Hcltech](#) contain the following vulnerability:

HCL Notes is susceptible to a stack based buffer overflow vulnerability in wp6sr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted WordPerfect file. This vulnerability applies to software previously licensed by IBM.

CVE-2022-44753 has been assigned by [HCL](#) psirt@hcl.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [HCL](#) **HCL Software** - **Notes** version = 9, 10

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Security Bulletin: IBM Notes is susceptible to multiple Micro Focus KeyView vulnerabilities (CVE-2022-44751, CVE-2022-44753, CVE-2022-44755) - Customer Support	support.hcltechsw.com text/html	MISC support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0100260

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Hcltech	Notes	10.0.1	-	All	All
Application	Hcltech	Notes	10.0.1	fp1	All	All
Application	Hcltech	Notes	10.0.1	fp2	All	All
Application	Hcltech	Notes	10.0.1	fp3	All	All
Application	Hcltech	Notes	10.0.1	fp4	All	All
Application	Hcltech	Notes	10.0.1	fp5	All	All
Application	Hcltech	Notes	10.0.1	fp6	All	All
Application	Hcltech	Notes	10.0.1	fp7	All	All
Application	Hcltech	Notes	9.0.1	-	All	All
Application	Hcltech	Notes	9.0.1	fp10	All	All
Application	Hcltech	Notes	9.0.1	fp10if1	All	All
Application	Hcltech	Notes	9.0.1	fp10if10	All	All
Application	Hcltech	Notes	9.0.1	fp10if2	All	All
Application	Hcltech	Notes	9.0.1	fp10if3	All	All
Application	Hcltech	Notes	9.0.1	fp10if4	All	All
Application	Hcltech	Notes	9.0.1	fp10if5	All	All
Application	Hcltech	Notes	9.0.1	fp10if6	All	All
Application	Hcltech	Notes	9.0.1	fp10if7	All	All
Application	Hcltech	Notes	9.0.1	fp10if8	All	All
Application	Hcltech	Notes	9.0.1	fp1if1	All	All
Application	Hcltech	Notes	9.0.1	fp1if2	All	All
Application	Hcltech	Notes	9.0.1	fp2if1	All	All
Application	Hcltech	Notes	9.0.1	fp2if2	All	All
Application	Hcltech	Notes	9.0.1	fp2if3	All	All
Application	Hcltech	Notes	9.0.1	fp2if4	All	All
Application	Hcltech	Notes	9.0.1	fp3if1	All	All
Application	Hcltech	Notes	9.0.1	fp3if2	All	All
Application	Hcltech	Notes	9.0.1	fp3if3	All	All
Application	Hcltech	Notes	9.0.1	fp3if4	All	All
Application	Hcltech	Notes	9.0.1	fp4if1	All	All
Application	Hcltech	Notes	9.0.1	fp4if2	All	All
Application	Hcltech	Notes	9.0.1	fp5if1	All	All
Application	Hcltech	Notes	9.0.1	fp5if2	All	All

Application	Hcltech	Notes	9.0.1	fp5if2	All	All
Application	Hcltech	Notes	9.0.1	fp5if3	All	All
Application	Hcltech	Notes	9.0.1	fp7if1	All	All
Application	Hcltech	Notes	9.0.1	fp7if2	All	All
Application	Hcltech	Notes	9.0.1	fp8if1	All	All
Application	Hcltech	Notes	9.0.1	fp9if1	All	All
Application	Hcltech	Notes	9.0.1	fp9if2	All	All
Application	Ibm	Notes	All	All	All	All
Application	Ibm	Notes	10.0.1	-	All	All
Application	Ibm	Notes	10.0.1	interim_fix_1	All	All
Application	Ibm	Notes	10.0.1	interim_fix_2	All	All
Application	Ibm	Notes	10.0.1	interim_fix_3	All	All
Application	Ibm	Notes	10.0.1	interim_fix_4	All	All
Application	Ibm	Notes	10.0.1	interim_fix_5	All	All
Application	Ibm	Notes	10.0.1	interim_fix_6	All	All
Application	Ibm	Notes	10.0.1	interim_fix_7	All	All
Application	Ibm	Notes	9.0.1.10	-	All	All
Application	Ibm	Notes	9.0.1.10	interim_fix_1	All	All
Application	Ibm	Notes	9.0.1.10	interim_fix_10	All	All
Application	Ibm	Notes	9.0.1.10	interim_fix_2	All	All
Application	Ibm	Notes	9.0.1.10	interim_fix_3	All	All
Application	Ibm	Notes	9.0.1.10	interim_fix_4	All	All
Application	Ibm	Notes	9.0.1.10	interim_fix_5	All	All
Application	Ibm	Notes	9.0.1.10	interim_fix_6	All	All
Application	Ibm	Notes	9.0.1.10	interim_fix_7	All	All
Application	Ibm	Notes	9.0.1.10	interim_fix_8	All	All
Application	Ibm	Notes	9.0.1.10	interim_fix_9	All	All
cpe:2.3:a:hcltech:notes:10.0.1:-:*:*:*:*:*:						
cpe:2.3:a:hcltech:notes:10.0.1:fp1:*:*:*:*:*:						
cpe:2.3:a:hcltech:notes:10.0.1:fp2:*:*:*:*:*:						
cpe:2.3:a:hcltech:notes:10.0.1:fp3:*:*:*:*:*:						
cpe:2.3:a:hcltech:notes:10.0.1:fp4:*:*:*:*:*:						
cpe:2.3:a:hcltech:notes:10.0.1:fp5:*:*:*:*:*:						
cpe:2.3:a:hcltech:notes:10.0.1:fp6:*:*:*:*:*:						

cpe:2.3:a:hcltech:notes:10.0.1:fp7:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:-::~~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp10:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp10if1:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp10if10:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp10if2:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp10if3:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp10if4:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp10if5:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp10if6:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp10if7:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp10if8:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp1if1:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp1if2:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp2if1:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp2if2:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp2if3:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp2if4:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp3if1:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp3if2:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp3if3:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp3if4:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp4if1:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp4if2:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp5if1:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp5if2:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp5if3:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp7if1:~::~~::~~::
cpe:2.3:a:hcltech:notes:9.0.1:fp7if2:~::~~::~~::

cpe:2.3:a:hcltech:notes:9.0.1:tp/it2:*:*:*:*:*:
cpe:2.3:a:hcltech:notes:9.0.1:fp8if1:*:*:*:*:*:
cpe:2.3:a:hcltech:notes:9.0.1:fp9if1:*:*:*:*:*:
cpe:2.3:a:hcltech:notes:9.0.1:fp9if2:*:*:*:*:*:
cpe:2.3:a:ibm:notes:*:*:*:*:*:
cpe:2.3:a:ibm:notes:10.0.1:-:*:*:*:*:
cpe:2.3:a:ibm:notes:10.0.1:interim_fix_1:*:*:*:*:
cpe:2.3:a:ibm:notes:10.0.1:interim_fix_2:*:*:*:*:
cpe:2.3:a:ibm:notes:10.0.1:interim_fix_3:*:*:*:*:
cpe:2.3:a:ibm:notes:10.0.1:interim_fix_4:*:*:*:*:
cpe:2.3:a:ibm:notes:10.0.1:interim_fix_5:*:*:*:*:
cpe:2.3:a:ibm:notes:10.0.1:interim_fix_6:*:*:*:*:
cpe:2.3:a:ibm:notes:10.0.1:interim_fix_7:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:-:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:interim_fix_1:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:interim_fix_10:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:interim_fix_2:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:interim_fix_3:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:interim_fix_4:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:interim_fix_5:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:interim_fix_6:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:interim_fix_7:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:interim_fix_8:*:*:*:*:
cpe:2.3:a:ibm:notes:9.0.1.10:interim_fix_9:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-44753 IBM Notes is susceptible to a stack based buffer overflow vulnera... twitter.com/i/web/status/1...	2022-12-17 02:55:55

 @CVEreport	CVE-2022-44753 : #IBM Notes is susceptible to a stack based buffer overflow vulnerability in wp6sr.dll in Micro Foc... twitter.com/i/web/status/1...	2022-12-19 11:11:22
 /r/netcve	CVE-2022-44753	2022-12-19 11:39:47

[< Previous ID](#)
[Next ID >](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)