Scan Report: couchbase:latest

Scan ID: 84627870-d38b-470c-ac9d-f168107b8406
Scan requested at: 2021-08-18T18:32:16Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 2, high - 7, medium - 15

Attack Vector: Network, Severity: Critical

CVE-2021-20231	
Vers: 3.6.13-2ubuntu1.3	Fix: 3.6.13-2ubuntu1.6
Name: gnutls28 Namespace: ubuntu:20.04 Description: A flaw was found in gnutls. A use after free issue in client sending key_share extension may lead to memory corruption and other consequences.	

CVE-2021-20232	
Vers: 3.6.13-2ubuntu1.3	Fix: 3.6.13-2ubuntu1.6
Name: gnutls28 Namespace: ubuntu:20.04 Description: A flaw was found in gnutls. A use after free issue in client_send_params in lib/ext/pre_shared_key.c may lead to memory corruption and other potential consequences.	

Attack Vector: Network, Severity: High

CVE-2017-11164	
Vers: 2:8.39-12build1	Fix: n/a
Name: pcre3 Namespace: ubuntu:20.04 Description: In PCRE 8.41, the OP_KETRMAX feature in the match function in pcre_exec.c allows stack exhaustion (uncontrolled recursion) when processing a crafted regular expression.	

CVE-2019-20838	
Vers: 2:8.39-12build1	Fix: n/a
Name: pcre3 Namespace: ubuntu:20.04 Description: libpcre in PCRE before 8.43 allows a subject buffer over-read in JIT when UTF is disabled, and \X or \R has more than one fixed quantifier, a related issue to CVE-2019-20454.	

Scan Report: couchbase:latest

Scan ID: 84627870-d38b-470c-ac9d-f168107b8406
Scan requested at: 2021-08-18T18:32:16Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 2, high - 7, medium - 15

CVE-2020-6096	
Vers: 2.31-0ubuntu9.2	Fix: n/a
Name: glibc Namespace: ubuntu:20.04 Description: An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.	

CVE-2021-3326	
Vers: 2.31-0ubuntu9.2	Fix: n/a
Name: glibc Namespace: ubuntu:20.04 Description: The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.	

CVE-2021-33560	
Vers: 1.8.5-5ubuntu1	Fix: n/a
Name: libgcrypt20 Namespace: ubuntu:20.04 Description: Libgcrypt before 1.8.8 and 1.9.x before 1.9.3 mishandles ElGamal encryption because it lacks exponent blinding to address a side-channel attack against mpi_powm, and the window size is not chosen appropriately. (There is also an interoperability problem because the selection of the k integer value does not properly consider the differences between basic ElGamal encryption and generalized ElGamal encryption.) This, for example, affects use of ElGamal in OpenPGP.	

SNYK-PYTHON-CRYPTOGRAPHY-1022152	
Vers: 3.4.6	Fix: n/a
Name: cryptography	

Scan Report: couchbase:latest

Scan ID: 84627870-d38b-470c-ac9d-f168107b8406
Scan requested at: 2021-08-18T18:32:16Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 2, high - 7, medium - 15

Namespace: {}
Description: n/a

Additional Findings

CVE-2013-4235	AV: local	Severity: medium
CVE-2016-10228	AV: network	Severity: medium
CVE-2016-2781	AV: local	Severity: medium
CVE-2018-1000654	AV: network	Severity: medium
CVE-2019-16167	AV: network	Severity: medium
CVE-2019-18276	AV: local	Severity: high
CVE-2019-25013	AV: network	Severity: medium
CVE-2020-14155	AV: network	Severity: medium
CVE-2020-27618	AV: local	Severity: medium
CVE-2020-29562	AV: network	Severity: medium
CVE-2021-31879	AV: network	Severity: medium
SNYK-JAVA-ORGAPACHECOMMONS-1316638	AV: network	Severity: medium
SNYK-JAVA-ORGAPACHECOMMONS-1316639	AV: network	Severity: medium
SNYK-JAVA-ORGAPACHECOMMONS-1316640	AV: network	Severity: medium
SNYK-JAVA-ORGAPACHECOMMONS-1316641	AV: network	Severity: medium
SNYK-PYTHON-URLLIB3-1533435	AV: network	Severity: medium