Deep Security
Smart Check

Scan Report: redis:latest

Scan ID: 58394947-df1f-4ebc-ab5c-506e8ccdb724
Scan requested at: 2021-08-18T18:25:50Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 5, high - 23, medium - 25

Attack Vector: Network, Severity: Critical

CVE-2005-2541	
Vers: 1.30+dfsg-6	Fix: n/a
Name: tar Namespace: debian:10 Description: Tar 1.15.1 does not properly warn the user when extracting setuid or setgid files, which may allow local users or remote attackers to gain privileges.	

CVE-2019-1010022	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: ** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."	

CVE-2019-9893	
Vers: 2.3.3-4	Fix: n/a
Name: libseccomp Namespace: debian:10 Description: libseccomp before 2.4.0 did not correctly generate 64-bit syscall argument comparisons using the arithmetic operators (LT, GT, LE, GE), which might able to lead to bypassing seccomp filters and potential privilege escalations.	

CVE-2021-33574	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or	

possibly unspecified other impact.

CVE-2021-35942	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atoi was used but strtoul should have been used to ensure correct calculations.	

Attack Vector: Network, Severity: High

CVE-2011-4116	
Vers: 5.28.1-6+deb10u1	Fix: n/a
Name: perl Namespace: debian:10 Description: _is_safe in the File::Temp module for Perl does not properly handle symlinks.	

CVE-2017-11164	
Vers: 2:8.39-12	Fix: n/a
Name: pcre3 Namespace: debian:10 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-2017-7245	
Vers: 2:8.39-12	Fix: n/a
Name: pcre3 Namespace: debian:10 Description: Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 4) or possibly have unspecified other impact via a crafted file.	

Scan Report: redis:latest

Scan ID: 58394947-df1f-4ebc-ab5c-506e8ccdb724
Scan requested at: 2021-08-18T18:25:50Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 5, high - 23, medium - 25

<table>
<tr><td colspan="2">CVE-2017-7246</td></tr>
<tr><td>Vers: 2:8.39-12</td><td>Fix: n/a</td></tr>
<tr><td colspan="2">Name: pcre3
Namespace: debian:10
Description: Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 268) or possibly have unspecified other impact via a crafted file.</td></tr>
</table>

<table>
<tr><td colspan="2">CVE-2018-12886</td></tr>
<tr><td>Vers: 8.3.0-6</td><td>Fix: n/a</td></tr>
<tr><td colspan="2">Name: gcc-8
Namespace: debian:10
Description: stack_protect_prologue in cfgexpand.c and stack_protect_epilogue in function.c in GNU Compiler Collection (GCC) 4.1 through 8 (under certain circumstances) generate instruction sequences when targeting ARM targets that spill the address of the stack protector guard, which allows an attacker to bypass the protection of -fstack-protector, -fstack-protector-all, -fstack-protector-strong, and -fstack-protector-explicit against stack overflow by controlling what the stack canary is compared against.</td></tr>
</table>

<table>
<tr><td colspan="2">CVE-2018-20796</td></tr>
<tr><td>Vers: 2.28-10</td><td>Fix: n/a</td></tr>
<tr><td colspan="2">Name: glibc
Namespace: debian:10
Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.</td></tr>
</table>

<table>
<tr><td colspan="2">CVE-2018-6829</td></tr>
<tr><td>Vers: 1.8.4-5+deb10u1</td><td>Fix: n/a</td></tr>
<tr><td colspan="2">Name: libgcrypt20
Namespace: debian:10
Description: cipher/elgamal.c in Libgcrypt through 1.8.2, when used to encrypt messages directly, improperly encodes plaintexts, which allows attackers to obtain sensitive information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). The Decisional Diffie-Hellman (DDH) assumption does not hold for Libgcrypt's ElGamal implementation.</td></tr>
</table>

Scan Report: redis:latest

Scan ID: 58394947-df1f-4ebc-ab5c-506e8ccdb724
Scan requested at: 2021-08-18T18:25:50Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 5, high - 23, medium - 25

CVE-2019-1010023	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: ** DISPUTED ** GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."	

CVE-2019-12290	
Vers: 2.0.5-1+deb10u1	Fix: n/a
Name: libidn2 Namespace: debian:10 Description: GNU libidn2 before 2.2.0 fails to perform the roundtrip checks specified in RFC3490 Section 4.2 when converting A-labels to U-labels. This makes it possible in some circumstances for one domain to impersonate another. By creating a malicious domain that matches a target domain except for the inclusion of certain punycoded Unicode characters (that would be discarded when converted first to a Unicode label and then back to an ASCII label), arbitrary domains can be impersonated.	

CVE-2019-14855	
Vers: 2.2.12-1+deb10u1	Fix: n/a
Name: gnupg2 Namespace: debian:10 Description: A flaw was found in the way certificate signatures could be forged using collisions found in the SHA-1 algorithm. An attacker could use this weakness to create forged certificate signatures. This issue affects GnuPG versions before 2.2.18.	

CVE-2019-15847	
Vers: 8.3.0-6	Fix: n/a
Name: gcc-8 Namespace: debian:10 Description: The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could	

optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same.

CVE-2019-17543	
Vers: 1.8.3-1+deb10u1	Fix: n/a
Name: lz4 Namespace: debian:10 Description: LZ4 before 1.9.2 has a heap-based buffer overflow in LZ4_write32 (related to LZ4_compress_destSize), affecting applications that call LZ4_compress_fast with a large input. (This issue can also lead to data corruption.) NOTE: the vendor states "only a few specific / uncommon usages of the API are at risk."	

CVE-2019-20838	
Vers: 2:8.39-12	Fix: n/a
Name: pcre3 Namespace: debian:10 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.	

CVE-2019-9192	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 Description: ** DISPUTED ** In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern.	

CVE-2019-9923	
Vers: 1.30+dfsg-6	Fix: n/a
Name: tar Namespace: debian:10	

Scan Report: redis:latest

Scan ID: 58394947-df1f-4ebc-ab5c-506e8ccdb724
Scan requested at: 2021-08-18T18:25:50Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 5, high - 23, medium - 25

Description: pax_decode_header in sparse.c in GNU Tar before 1.32 had a NULL pointer dereference when parsing certain archives that have malformed extended headers.

CVE-2020-6096	
Vers: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 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: 2.28-10	Fix: n/a
Name: glibc Namespace: debian:10 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.	

Additional Findings

CVE-2007-5686	AV: local	Severity: medium
CVE-2007-6755	AV: network	Severity: medium
CVE-2010-0928	AV: local	Severity: medium
CVE-2010-4051	AV: network	Severity: medium
CVE-2010-4052	AV: network	Severity: medium
CVE-2010-4756	AV: network	Severity: medium
CVE-2011-3389	AV: network	Severity: medium

Scan Report: redis:latest

Scan ID: 58394947-df1f-4ebc-ab5c-506e8ccdb724
Scan requested at: 2021-08-18T18:25:50Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 5, high - 23, medium - 25

CVE-2013-4235	AV: local	Severity: medium
CVE-2016-10228	AV: network	Severity: medium
CVE-2016-2781	AV: local	Severity: medium
CVE-2017-16231	AV: local	Severity: medium
CVE-2017-18018	AV: local	Severity: medium
CVE-2018-1000654	AV: network	Severity: medium
CVE-2018-7169	AV: network	Severity: medium
CVE-2019-1010024	AV: network	Severity: medium
CVE-2019-1010025	AV: network	Severity: medium
CVE-2019-13627	AV: local	Severity: medium
CVE-2019-18276	AV: local	Severity: high
CVE-2019-19882	AV: local	Severity: high
CVE-2019-25013	AV: network	Severity: medium
CVE-2019-3843	AV: local	Severity: high
CVE-2019-3844	AV: local	Severity: high
CVE-2020-10029	AV: local	Severity: medium
CVE-2020-13529	AV: local	Severity: medium
CVE-2020-13776	AV: local	Severity: medium
CVE-2020-14155	AV: network	Severity: medium
CVE-2020-1751	AV: local	Severity: high
CVE-2020-1752	AV: local	Severity: high
CVE-2020-27618	AV: local	Severity: medium
CVE-2021-20193	AV: network	Severity: medium
CVE-2021-37600	AV: local	Severity: medium