Improving FOSS Security

UbuCon Asia 2022

Nuritkum Square, Seoul, South Korea

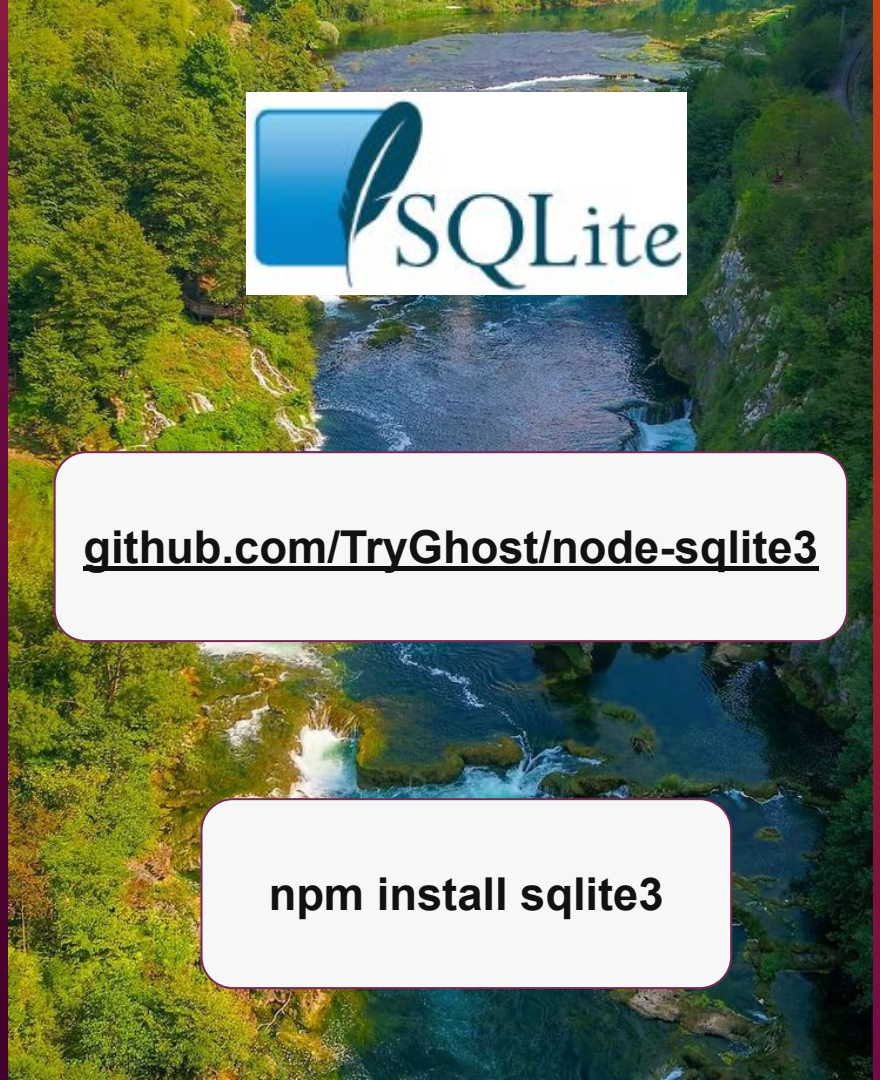
Mark Esler, Ubuntu Security Team

CANONICAL ubuntu

Part 1:

Background

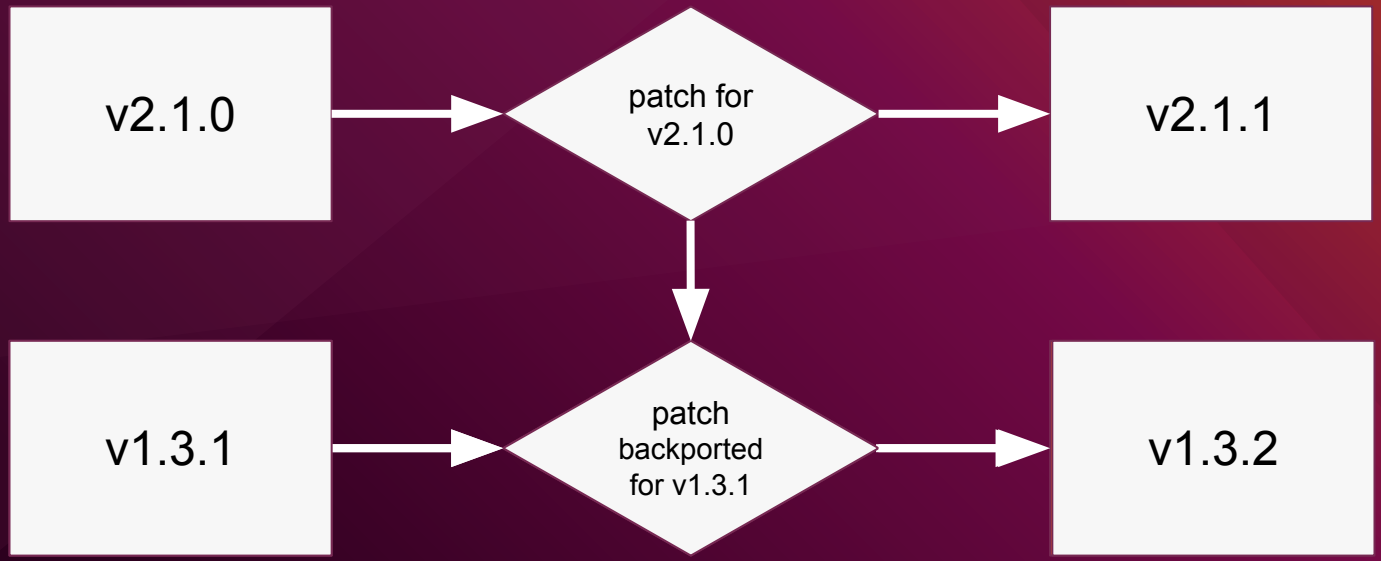
Upstream and Downstream



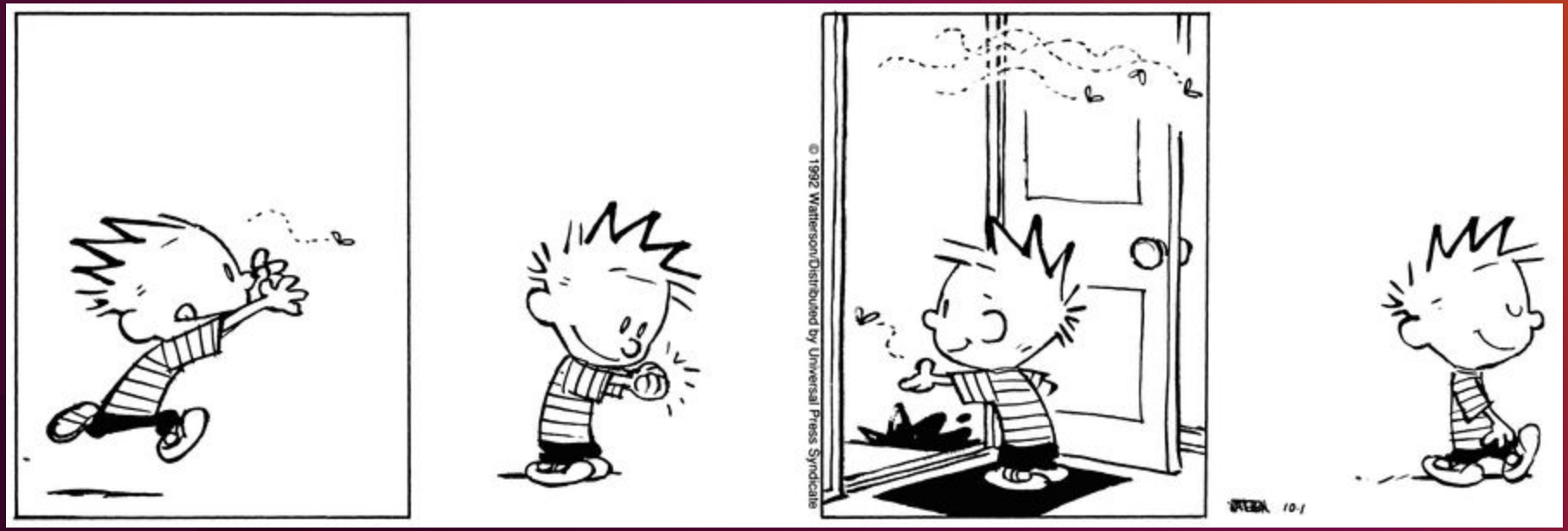
What do you call the person who finds a vulnerability?

Security Researcher / Reporter / Discoverer

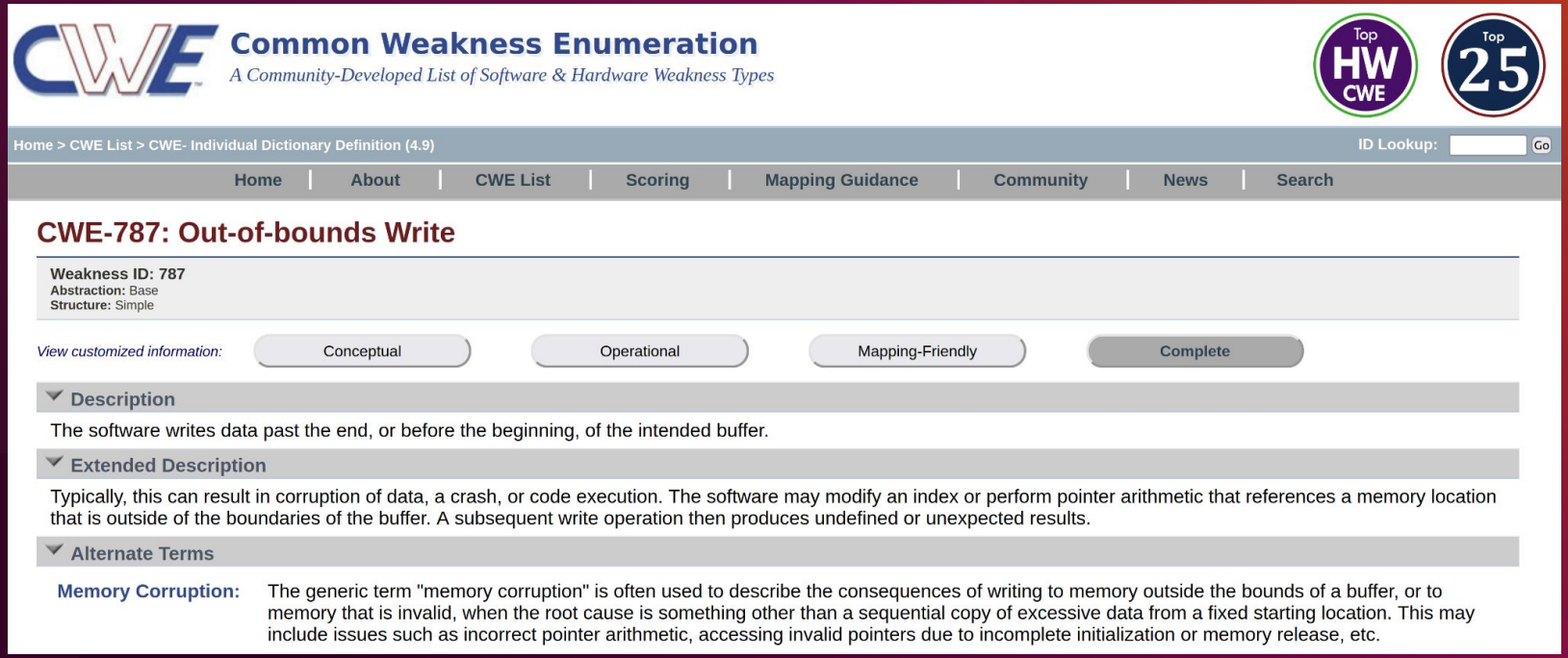
Backporting



Regression



Calvin and Hobbes by Bill Watterson for October 01, 1992



https://cwe.mitre.org/data/definitions/787.html

CVE-2021-44832

Published: **28 December 2021**

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

PRIORITY

Medium

CVSS 3 base score: 6.6

Status

PACKAGE	RELEASE	STATUS
apache-log4j2 Launchpad, Ubuntu, Debian	bionic	Released (2.12.4-0ubuntu0.1)
	focal	Released (2.17.1-0.20.04.1)
	hirsute	Released (2.17.1-0.21.04.1)
	impish	Released (2.17.1-0.21.10.1)
	jammy	Not vulnerable (2.17.1-1)

CVSS

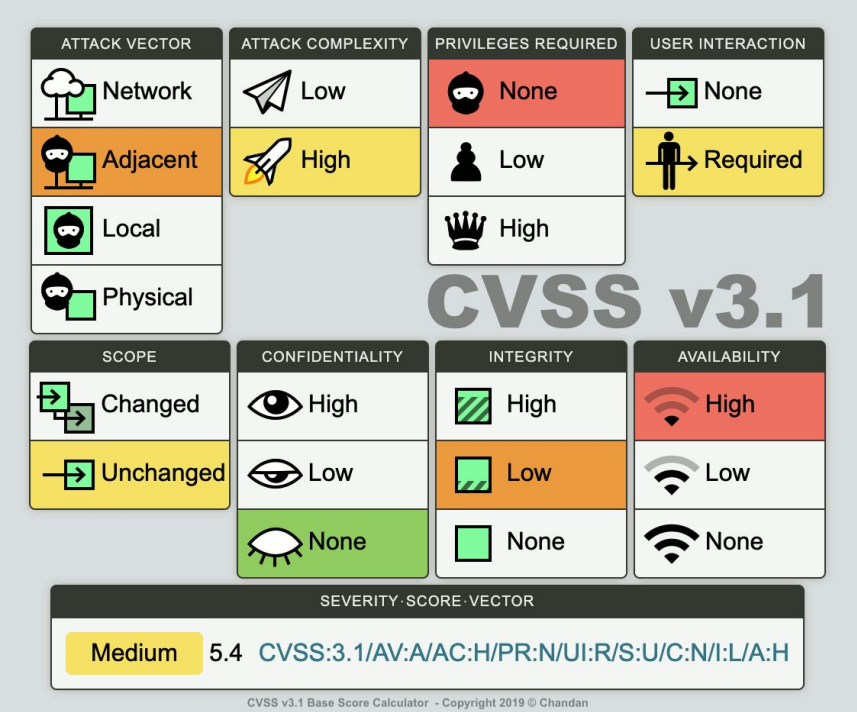
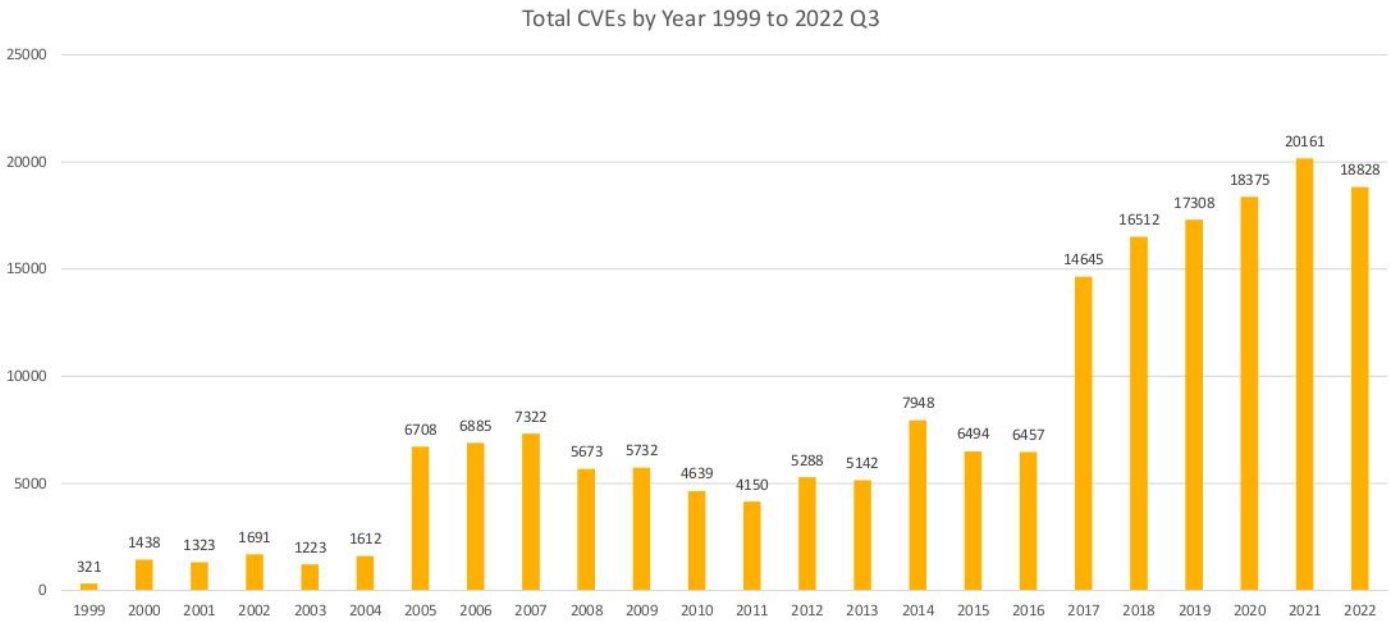


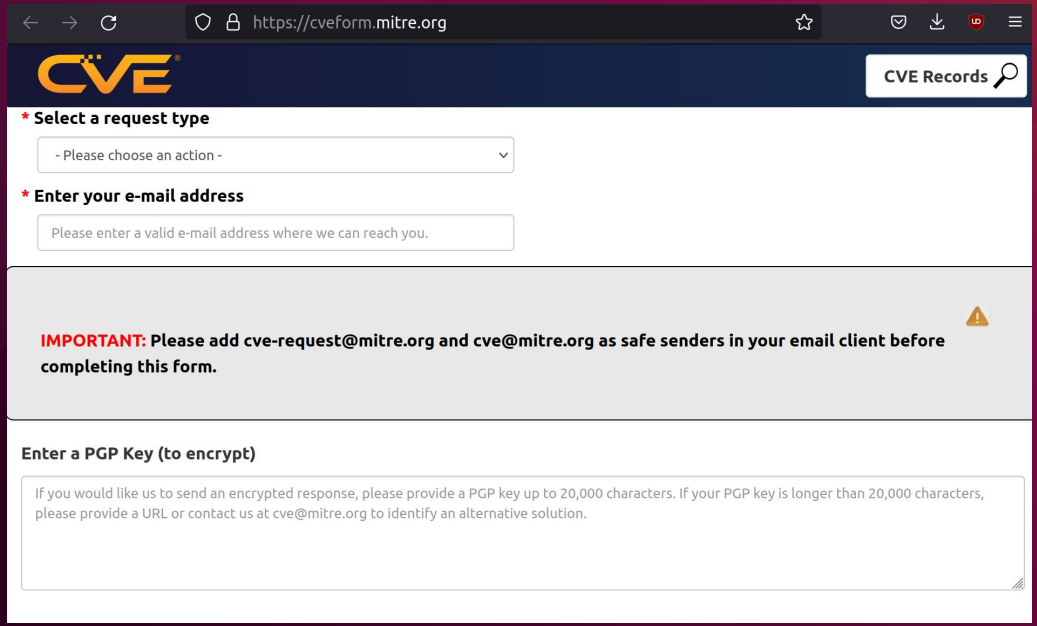
image from https://chandanbn.github.io/cvss/

CVE Numbers Growth



Slide from the CVE Program's "CVE Services Workshop" on November 2nd 2022. Shared with MITRE's permission.

Anyone can *request* a CVE



Key CVE Information

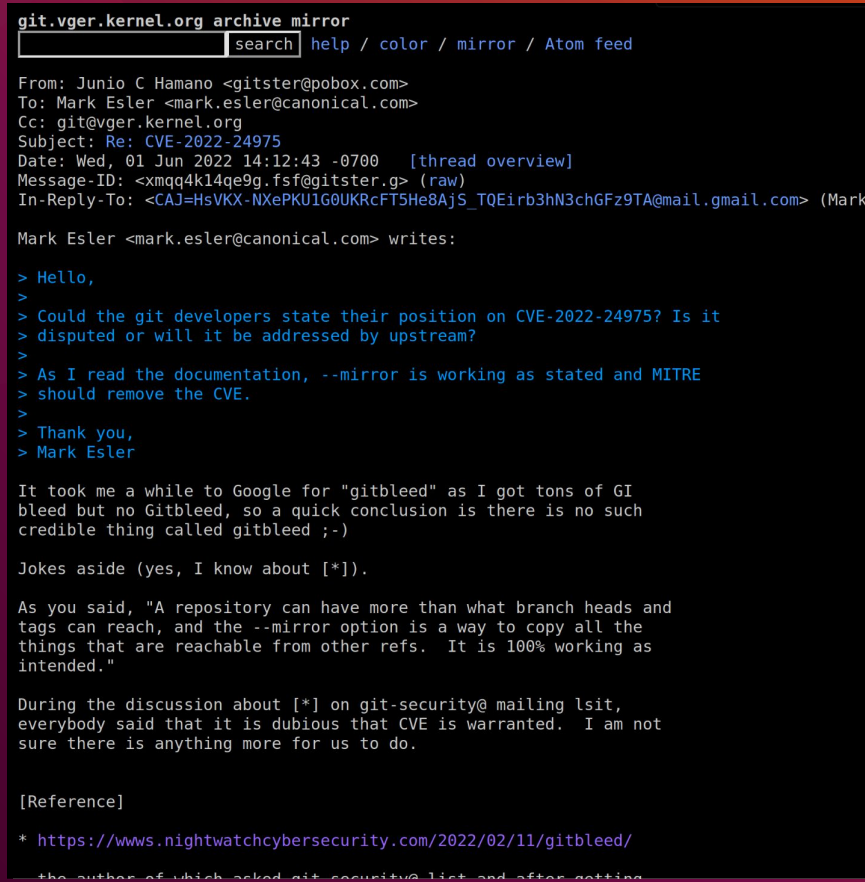
CVE-2021-44731 Detail

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	NIST Canonical Ltd.

Misassigned CVEs

- A CVE not considered a security issue by upstream



git.vger.kernel.org archive mirror

search help / color / mirror / Atom feed

From: Junio C Hamano <gitster@pobox.com>
To: Mark Esler <mark.esler@canonical.com>
Cc: git@vger.kernel.org
Subject: Re: CVE-2022-24975
Date: Wed, 01 Jun 2022 14:12:43 -0700 [thread overview]
Message-ID: <xmqq4k14qe9g.fsf@gitster.g> (raw)
In-Reply-To: <CAJ=HsVKX-NXePKU1G0UKRcFT5He8AjS_TQEirb3hN3chGFz9TA@mail.gmail.com> (Mark

Mark Esler <mark.esler@canonical.com> writes:

> Hello,
>
> Could the git developers state their position on CVE-2022-24975? Is it
> disputed or will it be addressed by upstream?
>
> As I read the documentation, --mirror is working as stated and MITRE
> should remove the CVE.
>
> Thank you,
> Mark Esler

It took me a while to Google for "gitbleed" as I got tons of GI
bleed but no Gitbleed, so a quick conclusion is there is no such
credible thing called gitbleed ;-)

Jokes aside (yes, I know about [*]).

As you said, "A repository can have more than what branch heads and
tags can reach, and the --mirror option is a way to copy all the
things that are reachable from other refs. It is 100% working as
intended."

During the discussion about [*] on git-security@ mailing lsit,
everybody said that it is dubious that CVE is warranted. I am not
sure there is anything more for us to do.

[Reference]

* https://wwws.nightwatchcybersecurity.com/2022/02/11/gitbleed/

the author of which asked git-security@ list and after getting

Misassigned CVEs

- A CVE not considered a security issue by upstream

CVE List▾ CNAs▾ WGs▾ Board▾ About▾ News & Blog▾

NVD
Go to for:
CVSS Scores
CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 188878

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)

NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.

HOME > CVE > CVE-2022-36640

Printer-Friendly View

CVE-ID

CVE-2022-36640 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

** DISPUTED ** influxData influxDB before v1.8.10 contains no authentication mechanism or controls, allowing unauthenticated attackers to execute arbitrary commands. NOTE: the CVE ID assignment is disputed because the vendor's documentation states "If InfluxDB is being deployed on a publicly accessible endpoint, we strongly recommend authentication be enabled. Otherwise the data will be publicly available to any unauthenticated user. The default settings do NOT enable authentication and authorization."

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

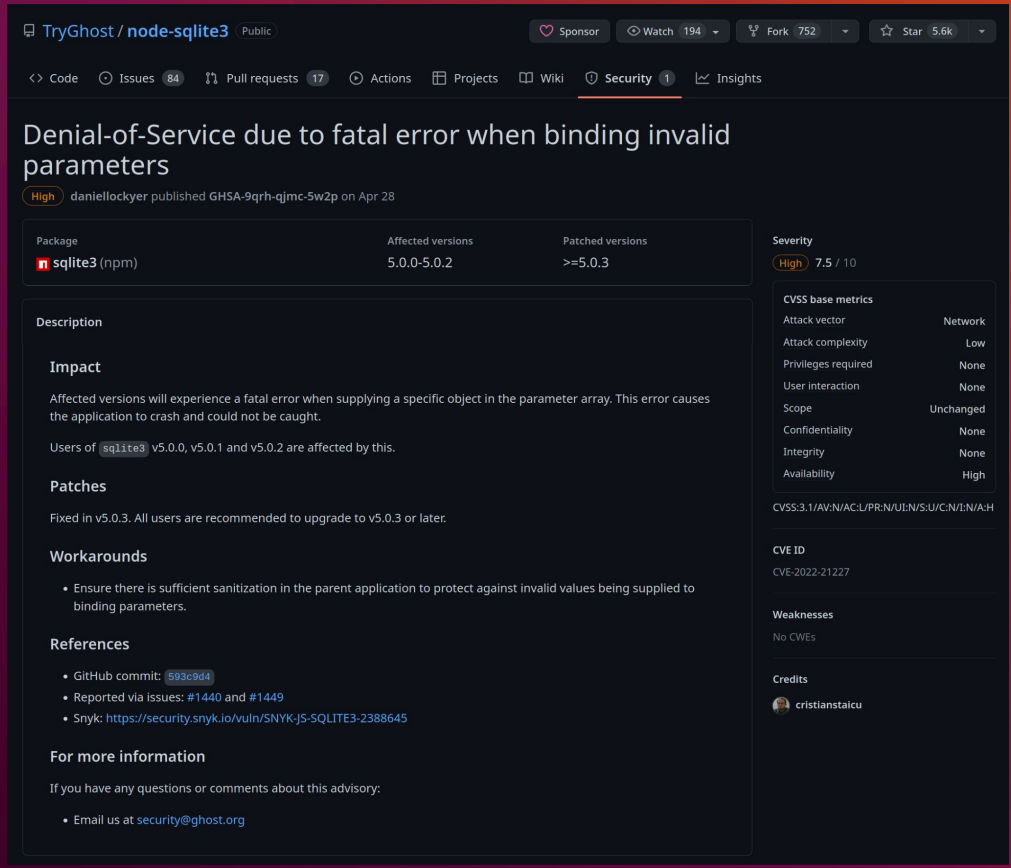
- MISC:http://influxdata.com
- MISC:http://influxdb.com
- MISC:http://www.krsecu.com/CVE/409b5310045bd6b9a984a5fb63bd8786d5c5681a8ad5b1c815c84b2b90002ad7.docx
- MISC:https://dl.influxdata.com/influxdb/releases/influxdb_1.8.10_amd64.deb
- MISC:https://portal.influxdata.com/downloads/
- MISC:https://www.influxdata.com/

Assigning CNA

MITRE Corporation

Misassigned CVEs

- A CVE in downstream assigned to upstream
- More examples: https://www.sqlite.org/cves.html



TryGhost / node-sqlite3 Public

Sponsor | Watch 194 | Fork 752 | Star 5.6k

Code | Issues 84 | Pull requests 17 | Actions | Projects | Wiki | Security 1 | Insights

Denial-of-Service due to fatal error when binding invalid parameters

High daniellockyer published GHSA-9qrh-qjmc-5w2p on Apr 28

Package	Affected versions	Patched versions
sqlite3 (npm)	5.0.0-5.0.2	>=5.0.3

Description

Impact

Affected versions will experience a fatal error when supplying a specific object in the parameter array. This error causes the application to crash and could not be caught.

Users of `sqlite3` v5.0.0, v5.0.1 and v5.0.2 are affected by this.

Patches

Fixed in v5.0.3. All users are recommended to upgrade to v5.0.3 or later.

Workarounds

- Ensure there is sufficient sanitization in the parent application to protect against invalid values being supplied to binding parameters.

References

- GitHub commit: `593c9d4`
- Reported via issues: #1440 and #1449
- Snyk: https://security.snyk.io/vuln/SNYK-JS-SQLITE3-2388645

For more information

If you have any questions or comments about this advisory:

- Email us at security@ghost.org

Severity

High 7.5 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2022-21227

Weaknesses

No CWEs

Credits

cristianstaicu

Misassigned CVEs

- A CVE that was assigned to a bug with no security impact

CVE-ID	
CVE-2022-3555	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.

Fix two memory leaks in _XFreeX11XCBStructure()

```
Even when XCloseDisplay() was called, some memory was leaked.

XCloseDisplay() calls _XFreeDisplayStructure(), which calls
_XFreeX11XCBStructure().

However, _XFreeX11XCBStructure() did not destroy the condition variables,
resulting in the leaking of some 40 bytes.

Signed-off-by: Hodong <hodong@yozmos.com>
```

https://git.launchpad.net/ubuntu-cve-tracker/

index : ubuntu-cve-tracker

[no description]

master switch

summary refs log tree commit diff

log msg search

Branch	Commit message	Author	Age
CVE-2021-37146	cve file syntax	florcabral	7 weeks
add-ros-esm-support	remove extra space	florcabral	5 weeks
addin_nvd_to_ubuntu_table_pkg_status	Adding --nvd priority filter to ubuntu-table and pkg_status scripts	Leonidas S. Barbosa	5 months
adding_special_ppas_flag	Adding special-ppa flag in order to handle ppas that are special for us and w...	Leonidas S. Barbosa	7 months
adding_this_only_affected_auto_info	Replacing cve_lib.subprojects for cve_lib.release_name	Leonidas S. Barbosa	7 months
cve_alert_nvd_score	Adding hability to list CVE affected packages by NVD priority	Leonidas S. Barbosa	5 months
making_this_only_opt	Making this_only_affected opt and fixing minor issues	Leonidas S. Barbosa	7 months
master	Process cves run: triaged 23 CVEs, 179 Ignored, 12 Packages	Paulo Flabiano Smorigo	**39 min.**
ros-esm	update supported packages for kinetic/melodic ros esm	florcabral	7 weeks
usns	usngrep: add reverse to --usns	Mark Esler	13 days

[...]

Tag	Download	Author	Age
v22.10	commit 82f0c65883...	Steve Beattie	3 weeks
v22.04	commit a3397479bb...	Steve Beattie	7 months
jammy-open	commit 396cf2a3f7...	Steve Beattie	13 months
v21.10	commit 53f69111bc...	Steve Beattie	13 months
git-conversion	commit dc3f64a0df...	Steve Beattie	4 years

Age	Commit message	Author
39 min.	Process cves run: triaged 23 CVEs, 179 Ignored, 12 Packages HEAD master	Paulo Flabiano Smorigo
5 hours	merge cve updates from kernel team	Steve Beattie
5 hours	CVE-2022-37290: looks like caja may be affected as well	Steve Beattie
6 hours	kernel/CVE-2022-3623: autotriage	Thadeu Lima de Souza Cascardo
6 hours	kernel/CVE-2022-3636: add description	Thadeu Lima de Souza Cascardo
7 hours	kernel/CVE-2022-3640: add description	Thadeu Lima de Souza Cascardo
7 hours	kernel/CVE-2022-3545: add description	Thadeu Lima de Souza Cascardo
7 hours	kernel/CVE-2022-3541: add description	Thadeu Lima de Souza Cascardo
7 hours	kernel/CVE-2022-3526: add description	Thadeu Lima de Souza Cascardo
7 hours	ldap-account-manager/CVE-2018-8764: retriage CVE	Steve Beattie

[...]

Clone

git://git.launchpad.net/ubuntu-cve-tracker

git+ssh://git.launchpad.net/ubuntu-cve-tracker

https://git.launchpad.net/ubuntu-cve-tracker

Vulnerability Disclosure

See OpenSSF's Preparing for Zero-Day

Security Maintenance

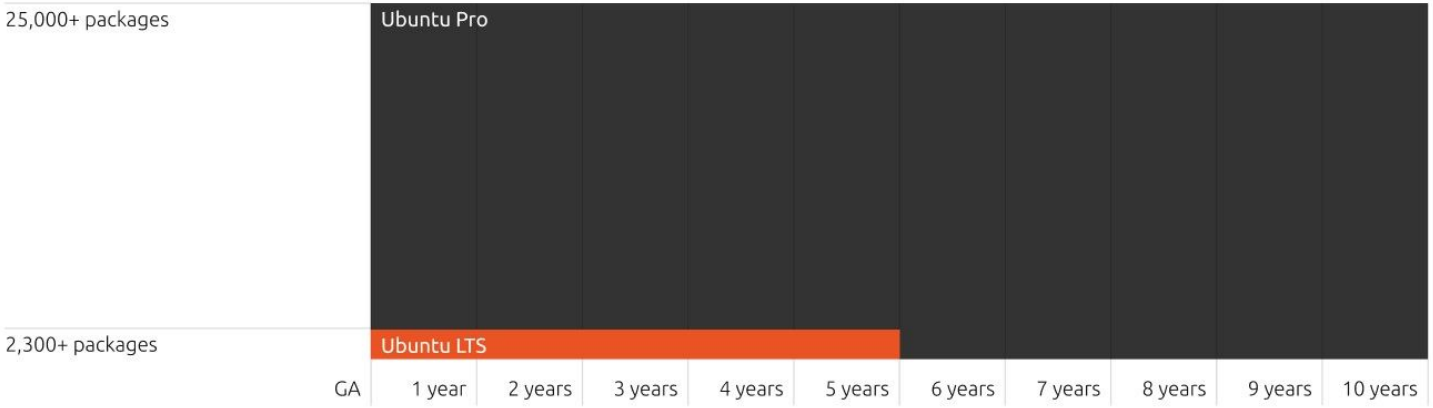
- Reactively close vulnerabilities
- Track and address vulnerabilities
- Coordinate with upstream
- Apply and backport patches

Part 2:

Ubuntu Security Maintenance

What's the difference?

SECURITY PATCHING (Coverage for critical, high and selected medium CVEs)	UBUNTU LTS	UBUNTU PRO (INFRA-ONLY) (Previously known as "Ubuntu Advantage for Infrastructure")	UBUNTU PRO
Over 2,300 packages in Ubuntu Main repository	5 years	10 years	10 years
Over 23,000 packages in Ubuntu Universe repository	Best effort	Best effort	10 years



Step 1: Initial Triage

- Determine what is affected
- Determine severity
- Determine response

```
PublicDateAtUSN: 2021-12-10 00:00:00 UTC
Candidate: CVE-2021-44228
PublicDate: 2021-12-10 10:15:00 UTC
References:
 https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/Log4Shell
 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
 https://github.com/apache/logging-log4j2/pull/608
 https://github.com/apache/logging-log4j2/commit/c77b3cb39312b83b053d23a2158b99ac7de44dd3
 https://github.com/tangxiaofeng7/apache-log4j-poc
 https://github.com/advisories/GHSA-jfh8-c2jp-5v3q
 https://ubuntu.com/security/notices/USN-5192-1
 https://ubuntu.com/security/notices/USN-5197-1
 https://ubuntu.com/security/notices/USN-5192-2
Description:
 Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2,
 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and
 parameters do not protect against attacker controlled LDAP and other JNDI
 related endpoints. An attacker who can control log messages or log message
 parameters can execute arbitrary code loaded from LDAP servers when message
 lookup substitution is enabled. From log4j 2.15.0, this behavior has been
 disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and
 2.3.1), this functionality has been completely removed. Note that this
 vulnerability is specific to log4j-core and does not affect log4net,
 log4cxx, or other Apache Logging Services projects.
Ubuntu-Description:
Notes:
 mdeslaur> apache-log4j1.2 contains a similar issue in a non-default
  configuration, and it was assigned CVE-2021-4104, see that CVE for
  information about apache-log4j1.2
Bugs:
Priority: high
Discovered-by: Chen Zhaojun
Assigned-to: pfsmorigo
CVSS:
 asf: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H [10.0 CRITICAL]
 nvd: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H [10.0 CRITICAL]

Patches_apache-log4j2:
 upstream: https://github.com/apache/logging-log4j2/commit/c77b3cb39312b83b053d23a2158b99ac7de44dd3
upstream_apache-log4j2: released (2.15.0)
trusty_apache-log4j2: ignored (out of standard support)
trusty/esm_apache-log4j2: DNE
xenial_apache-log4j2: ignored (out of standard support)
esm-infra/xenial_apache-log4j2: released (2.4-2ubuntu0.1~esm1)
bionic_apache-log4j2: released (2.10.0-2ubuntu0.1)
focal_apache-log4j2: released (2.15.0-0.20.04.1)
hirsute_apache-log4j2: released (2.15.0-0.21.04.1)
impish_apache-log4j2: released (2.15.0-0.21.10.1)
jammy_apache-log4j2: not-affected (2.15.0-1)
devel_apache-log4j2: not-affected (2.15.0-1)
```

Step 2: Patching

- Patch specific research
- Backport patch to older releases

```
--- apache-log4j2-2.10.0.orig/log4j-core/src/main/java/org/apache/logging/log4j/core/lookup/JndiLookup.java
+++ /dev/null
@@ -1,76 +0,0 @@
-/*
- * Licensed to the Apache Software Foundation (ASF) under one or more
- * contributor license agreements. See the NOTICE file distributed with
- * this work for additional information regarding copyright ownership.
- * The ASF licenses this file to You under the Apache license, Version 2.0
- * (the "License"); you may not use this file except in compliance with
- * the License. You may obtain a copy of the License at
- *
- *      http://www.apache.org/licenses/LICENSE-2.0
- *
- * Unless required by applicable law or agreed to in writing, software
- * distributed under the License is distributed on an "AS IS" BASIS,
- * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
- * See the license for the specific language governing permissions and
- * limitations under the license.
- */
-package org.apache.logging.log4j.core.lookup;
-
-import java.util.Objects;
-
-import javax.naming.NamingException;
-
-import org.apache.logging.log4j.Logger;
-import org.apache.logging.log4j.Marker;
-import org.apache.logging.log4j.MarkerManager;
-import org.apache.logging.log4j.core.LogEvent;
-import org.apache.logging.log4j.core.config.plugins.Plugin;
-import org.apache.logging.log4j.core.net.JndiManager;
-import org.apache.logging.log4j.status.StatusLogger;
-
-/**
- * Looks up keys from JNDI resources.
- */
-@Plugin(name = "jndi", category = StrLookup.CATEGORY)
-public class JndiLookup extends AbstractLookup {
-
-    private static final Logger LOGGER = StatusLogger.getLogger();
-    private static final Marker LOOKUP = MarkerManager.getMarker("LOOKUP");
-
-    /** JNDI resource path prefix used in a J2EE container */
-    static final String CONTAINER_JNDI_RESOURCE_PATH_PREFIX = "java:comp/env/";
-
-    /**
-     * Looks up the value of the JNDI resource.
-     * @param event The current LogEvent (is ignored by this StrLookup).
-     * @param key  the JNDI resource name to be looked up, may be null
-     * @return The String value of the JNDI resource.
-     */
-    @Override
-    public String lookup(final LogEvent event, final String key) {
-        if (key == null) {
-            return null;
-        }
-        final String jndiName = convertJndiName(key);
-        try (final JndiManager jndiManager = JndiManager.getDefaultManager()) {
-            return Objects.toString(jndiManager.lookup(jndiName), null);
-        } catch (final NamingException e) {
```

Step 3: Changelog

```
apache-log4j2 (2.10.0-2ubuntu0.1) bionic-security; urgency=medium

  * SECURITY UPDATE: Remote code execution
    - debian/patches/CVE-2021-44228.patch: Remove JndiLookup class.
    - CVE-2021-44228

 -- Paulo Flabiano Smorigo <pfsmorigo@canonical.com>  Fri, 10 Dec 2021 17:24:48 +0000
```

Step 4: Patch Testing

- Compare build logs and run internal tools
- Test local and Launchpad builds
- Test against vulnerability

README.md

CVE-2021-44228(Apache Log4j Remote Code Execution)

> all log4j-core versions >=2.0-beta9 and <=2.14.1

The version of 1.x have other vulnerabilities, we recommend that you update the latest version.

Security Advisories / Bulletins linked to Log4Shell (CVE-2021-44228)

Usage:

download this project, compile the exploit code blob/master/src/main/java/Exploit.java, and start a webserver allowing downloading the compiled binary.

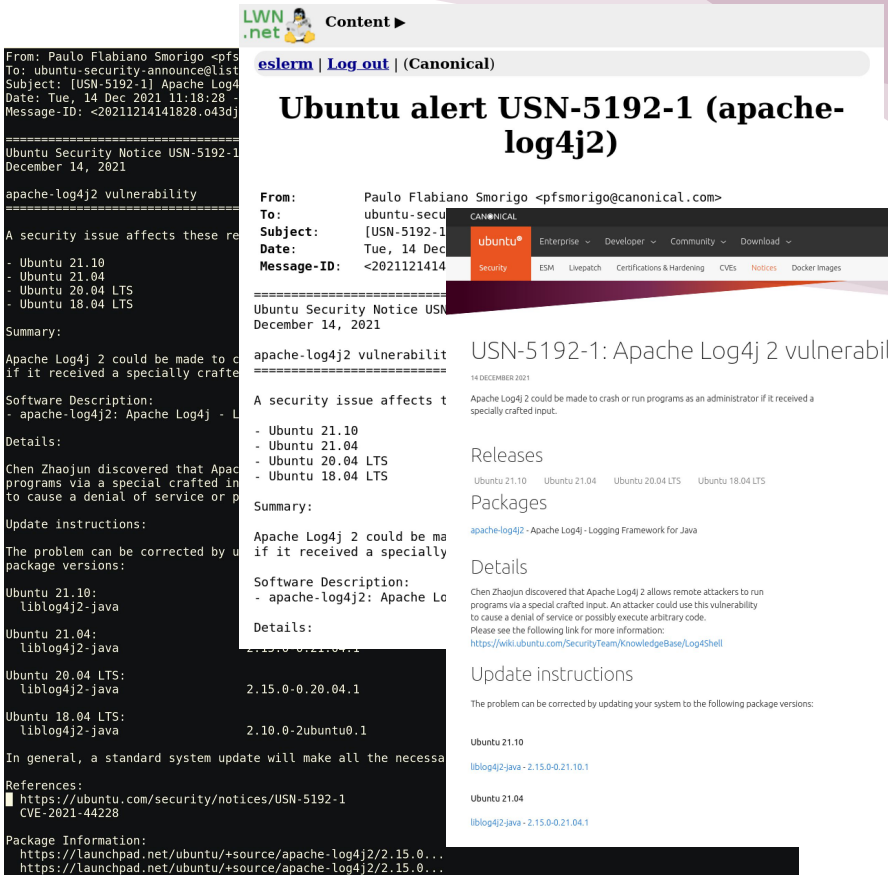
```
git clone https://github.com/tangxiaofeng7/CVE-2021-44228-Apache-Log4j-Rce.git
cd CVE-2021-44228-Apache-Log4j-Rce

javac Exploit.java

# start webserver
# For Python2
python -m SimpleHTTPServer 8888
# For Python3
python3 -m http.server 8888

# make sure python webserver is running the same directory as Exploit.class, to test
  curl -I 127.0.0.1:8888/Exploit.class
```

download another project and run *LDAP server implementation returning JNDI references* https://github.com/mbechler/marshalsec/blob/master/src/main/java/marshalsec/jndi/LDAPRefServer.java

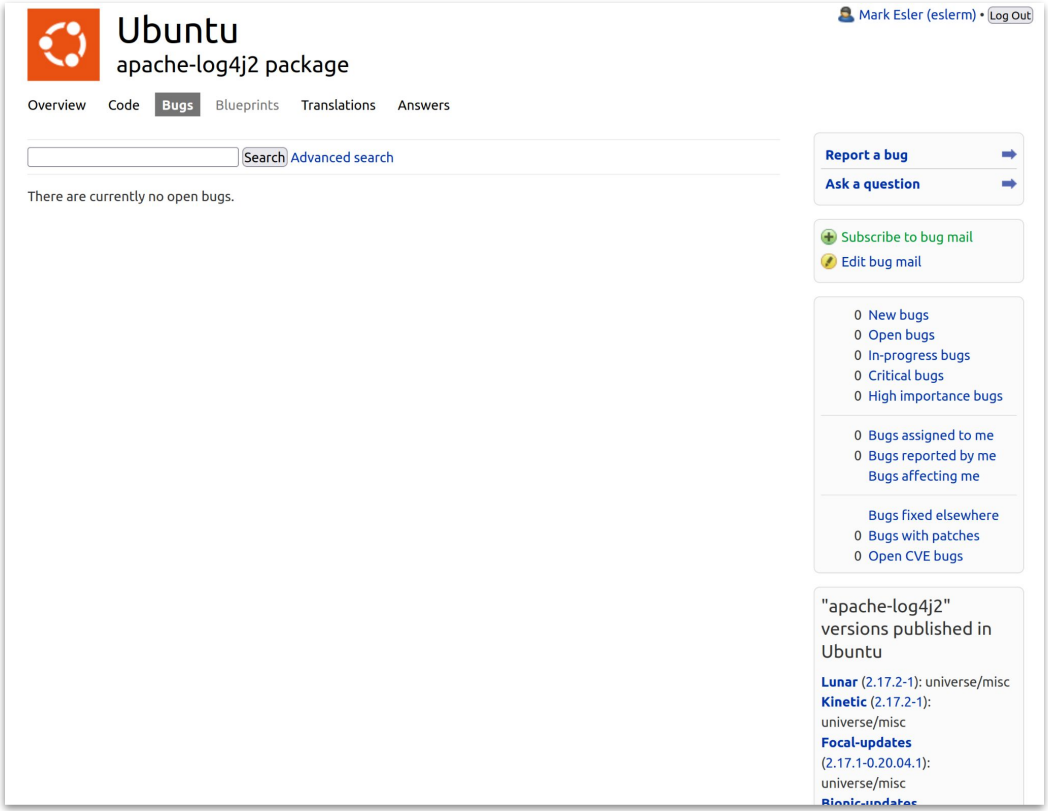
```
git clone https://github.com/mbechler/marshalsec.git
cd marshalsec
```

Step 5: Publication and Announcement

- Publish package to Ubuntu Archive
- Announced by email
- Re-published on Ubuntu website and by third-parties



Step 6: Monitor Feedback



Part 3:

Improving FOSS Security

You Retweeted

Formal Ferris
@FormalFerris

hot tip: to avoid writing bugs, don't write software

9:09 PM · Jun 4, 2022 · Twitter Web App

1,767 Retweets **176** Quote Tweets **14.7K** Likes

It is okay to disclose vulnerabilities.

(* ^ _ ^) ノ

Use After Free in function did_set_string_option fix in vim - Sep 28

Stack-based Buffer Overflow in function win_redr_ruler fix in vim - Sep 26

Use After Free in function process_next_cpt_value fix in vim - Sep 24

Stack-based Buffer Overflow in function ex_finally fix in vim - Sep 24

Access violation near NULL on destination operand eval.c:2603:37 in segmentation fault fix in vim - Sep 22

Use After Free in function movemark fix in vim - Sep 21

Use After Free in function getcmdline_int fix in vim - Sep 17

Heap-based Buffer Overflow in function utfc_ptr2len fix in vim - Sep 16

Null Dereference in vim_regcomp() fix in vim - Sep 7

Use After Free in function do_tag fix in vim - Sep 5

Use After Free in function do_cmdline fix in vim - Sep 2

Use After Free in Function qf_buf_add_line() fix in vim - Aug 29

Use After Free in function get_next_valid_entry fix in vim - Aug 27

Use After Free in function qf_fill_buffer fix in vim - Aug 24

NULL Pointer Dereference in function do_mouse fix in vim - Aug 24

Use After Free in function vim_vsnprintf_typval fix in vim - Aug 22

NULL Pointer Dereference in function sug_filltree fix in vim - Aug 21

Use After Free in function find_var_also_in_script fix in vim - Aug 18

NULL Pointer Dereference in function generate_loadvar fix in vim - Aug 17

use after free in function generate_PCALL fix in vim - Aug 16

Heap-based Buffer Overflow in function latin_ptr2len fix in vim - Aug 16

Buffer Over-read in function utf_head_off fix in vim - Aug 16

Use After Free in function string_quote fix in vim - Aug 14

Out-of-bounds read in function check_vim9_unlet in vim/vim fix in vim - Aug 14

Heap-based Buffer Overflow in function compile_lock_unlock in vim/vim fix in vim - Aug 14

Undefined behavior in diff_write_buffer() fix in vim - Jul 30

Out-of-bounds Read in function utf_ptr2char fix in vim - Jul 29

heap-buffer-overflow occurs in function eval_string ./vim/src/typval.c:2226 fix in vim - Jul 29

Heap-based buffer overflow in function vim_iswordp_buf fix in vim - Jul 28

Heap-based Buffer Overflow in function ins_compl_infercase_gettext() fix in vim - Jul 23

Heap Use After Free in function skipwhite fix in vim - Jul 7

Heap-based buffer overflow in function ins_compl_add fix in vim - Jul 7

Heap-based Buffer Overflow in function ins_compl_add fix in vim - Jul 7

Stack-based Buffer Overflow in function spell_dump_compl fix in vim - Jul 4

Heap Use After Free in function ex_diffgetput fix in vim - Jul 2

Out-of-bound write in function parse_command_modifiers fix in vim - Jul 2

Out-of-bound read data in function suggest_trie_walk() abusing array byts fix in vim - Jul 1

Out-of-bounds Read in function ins_bytes fix in vim - Jul 1

Integer Overflow in function del_typebuf fix in vim - Jul 1

Heap-based Buffer Overflow in function utfc_ptr2len fix in vim - Jul 1

Heap-based buffer overflow in function inc fix in vim - Jun 30

Out-of-bound read in function msg_outtrans_special fix in vim - Jun 29

Null pointer dereference in function skipwhite fix in vim - Jun 27

Out-of-bound write in function ml_append_int fix in vim - Jun 26

Null pointer dereference in function diff_check fix in vim - Jun 26

Heap-based buffer overflow in function ins_bs fix in vim - Jun 26

Out-of-bound read in function msg_outtrans_attr fix in vim - Jun 25

Out-of-bounds Read in function get_lisp_indent fix in vim - Jun 22

Heap-based Buffer Overflow in function utf_ptr2char fix in vim - Jun 22

Buffer Over-read in function put_on_cmdline fix in vim - Jun 22

Memory leaks in function vim_strsave fix in vim - Jun 21

Out-of-bounds write in function vim_regsub_both fix in vim - Jun 18

Out-of-bounds Read in function suggest_trie_walk fix in vim - Jun 18

Heap-based Buffer Overflow in function get_lisp_indent fix in vim - Jun 18

Buffer Over-read in function current_quote fix in vim - Jun 18

use after free in skipwhite fix in vim - Jun 9

Out-of-bounds write in function append_command fix in vim - Jun 6

Use After Free in function utf_ptr2char fix in vim - Jun 1

Heap-based Buffer Overflow in function vim_regsub_both fix in vim - May 30

Buffer Over-read in function utf_ptr2char fix in vim - May 28

Use After Free in function find_pattern_in_path fix in vim - May 26

Out-of-bounds write in function vim_regsub_both fix in vim - May 26

Heap-based Buffer Overflow in function utf_head_off fix in vim - May 25

Out-of-bounds read in function gchar_cursor fix in vim - May 24

heap-use-after-free in function find_pattern_in_path fix in vim - May 18

Out-of-bounds write in function vim_regsub_both fix in vim - May 18

Infinite recursive function calls result in stack overflow fix in vim - May 17

Buffer Over-read in function get_one_sourceline fix in vim - May 17

Buffer Over-read in function utfc_ptr2len fix in vim - May 16

Heap-based Buffer Overflow in function skip_string fix in vim - May 16

NULL Pointer Dereference in function vim_regexec_string fix in vim - May 15

Buffer Over-read in function grab_file_name fix in vim - May 14

NULL Pointer Dereference in function vim_regexec_string at regexp.c:2733 fix in vim - May 11

Buffer Over-read in function find_next_quote fix in vim - May 9

Heap buffer overflow in vim_strncpy find_word fix in vim - May 8

NULL Pointer Dereference in function vim_regexec_string at regexp.c:2729 fix in vim - May 7

Heap-based Buffer Overflow in function cmdline_erase_chars fix in vim - May 7

Use after free in append_command fix in vim - May 6

Use of Out-of-range Pointer Offset fix in vim - Apr 17

global heap buffer overflow in skip_range fix in vim - Apr 16

heap buffer overflow in get_one_sourceline fix in vim - Mar 29

Use after free in utf_ptr2char fix in vim - Mar 29

Heap-based Buffer Overflow occurs in vim fix in vim - Mar 13

Use of Out-of-range Pointer Offset fix in vim - Feb 22

Heap-based Buffer Overflow fix in vim - Feb 21

NULL Pointer Dereference fix in vim - Feb 20

Use of Out-of-range Pointer Offset fix in vim - Feb 19

Stack-based Buffer Overflow fix in vim - Feb 16

Heap-based Buffer Overflow fix in vim - Feb 12

Use of Out-of-range Pointer Offset fix in vim - Feb 9

Floating Point Comparison with Incorrect Operator fix in vim - Feb 5

Use After Free fix in vim - Feb 1

Heap-based Buffer Overflow fix in vim - Jan 30

Use After Free fix in vim - Jan 29

Stack-based Buffer Overflow fix in vim - Jan 28

Heap-based Buffer Overflow fix in vim - Jan 28

Out-of-bounds Read fix in vim - Jan 27

Heap-based Buffer Overflow fix in vim - Jan 27

Out-of-bounds Read fix in vim - Jan 25

Heap-based Buffer Overflow fix in vim - Jan 25

Heap-based Buffer Overflow fix in vim - Jan 25

Access of Memory Location Before Start of Buffer fix in vim - Jan 24

Out-of-bounds Read fix in vim - Jan 20

Heap-based Buffer Overflow fix in vim - Jan 20

Heap-based Buffer Overflow fix in vim - Jan 17

Heap-based Buffer Overflow fix in vim - Jan 13

Allocation of Resources Without Limits or Throttling fix in vim - Jan 11

Heap-based Buffer Overflow fix in vim - Jan 9

Use After Free fix in vim - Jan 8

Out-of-bounds Read fix in vim - Jan 5

Out-of-bounds Read fix in vim - Dec 30

Use After Free fix in vim - Dec 30

Use After Free fix in vim - Dec 28

Use After Free fix in vim - Dec 26

Out-of-bounds Read fix in vim - Dec 24

Untrusted Pointer Dereference fix in vim - Dec 24

Heap-based Buffer Overflow fix in vim - Dec 18

Use After Free fix in vim - Dec 5

Heap-based Buffer Overflow fix in vim - Nov 25

Heap-based Buffer Overflow fix in vim - Nov 19

Use After Free fix in vim - Nov 17

Heap-based Buffer Overflow fix in vim - Nov 17

Heap-based Buffer Overflow fix in vim - Nov 17

Use of Uninitialized Variable fix in vim - Nov 4

Heap-based Buffer Overflow fix in vim - Nov 4

Heap-based Buffer Overflow fix in vim - Oct 25

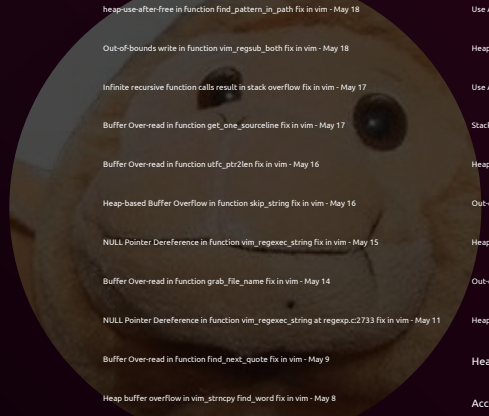
Heap-based Buffer Overflow fix in vim - Oct 9

Heap-based Buffer Overflow fix in vim - Oct 8

Use After Free fix in vim - Sep 11

Heap-based Buffer Overflow fix in vim - Sep 7

Heap-based Buffer Overflow fix in vim - Sep 5



There are no security specific releases of kitty. Security bugs are fixed and released just like all other bugs.

- https://github.com/kovidgoyal/kitty/blob/master/SECURITY.md

Bram Moolenaar

brammool

Follow

Author of Vim, A-a-p and Zimbu.

2.1k followers · **0** following

Zimbu Labs
Tenerife, Spain
bram@moolenaar.net
http://www.moolenaar.net

Achievements

x3 x4

Beta Send feedback

Organizations

Block or Report

Overview | Repositories 2 | Projects | Packages | Stars

Popular repositories

vim9 — Public archive
Forked from vim/vim
An experimental fork of Vim, exploring ways to make Vim script faster and better.
Vim Script · 475 · 17

libvterm — Public
Forked from neovim/libvterm
Mirror of http://bazaar.leonerd.org.uk/c/libvterm/
C · 4 · 3

1,775 contributions in the last year

Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov

Mon
Wed
Fri

Learn how we count contributions

Less More

Contribution activity

2022
2021
2020
2019
2018
2017
2016
2015
2014

November 2022

Created 37 commits in 1 repository
vim/vim 37 commits

Reviewed 1 pull request in 1 repository
vim/vim
1 pull request
Fix 'eof' option
Nov 1

Show more activity

Seeing something unexpected? Take a look at the GitHub profile guide.

It is okay to disclose vulnerabilities.

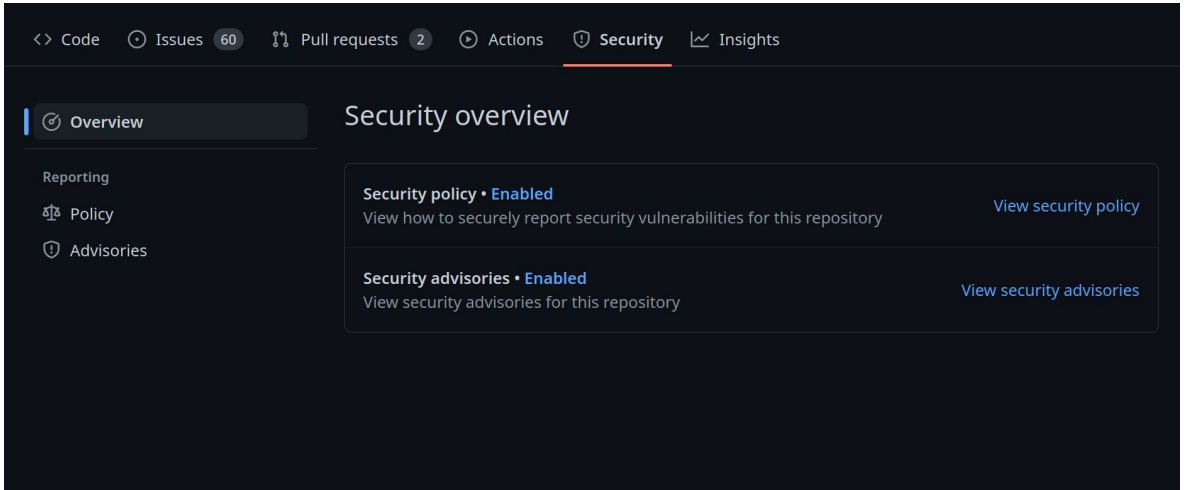
(* ^ _ ^) ノ

Write a Security Policy.

(*^ – ^)ノ

Write a Security Policy

- Explain to researchers how they can report vulnerabilities to you.
- *“If you find a vulnerability email me@abc.xyz”* is much better than nothing!



OpenSSF Security Policy

- OpenSSF has excellent guides!

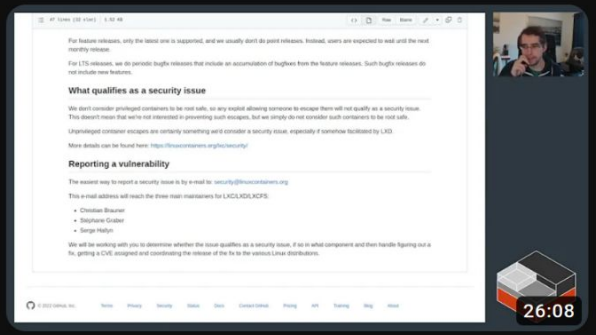
SECURITY.MD for GitHub Security Policy

To report a security issue, please email $VMTalias with a description of the issue, the steps you took to create the issue, affected versions, and, if known, mitigations for the issue. Our vulnerability management team will respond within 3 working days of your email. If the issue is confirmed as a vulnerability, we will open a Security Advisory. This project follows a 90 day disclosure timeline.

https://github.com/ossf/oss-vulnerability-guide/blob/main/templates/security_policies/github_security_policy.md

LXD Security Policy

- Documents application security



LXD security

212 views • 5 days ago

LXD

Let's look at **LXD's** security story. Not just how to make running instances safer but also the general **security policy** for the project ...

New

Introduction | Demo | Conclusion 3 chapters

SECURITY.md

Security policy

Supported versions

LXD has two types of releases:

- Monthly feature releases
- LTS releases

For feature releases, only the latest one is supported, and we usually don't do point releases.

Reporting a vulnerability

The easiest way to report a security issue is by e-mail to: security@linuxcontainers.org

This e-mail address will reach the three main maintainers for LXC/LXD/LXCFS:

- Christian Brauner
- Stéphane Graber
- Serge Hallyn

We will be working with you to determine whether the issue qualifies as a security issue, if so in what component and then handle figuring out a fix, getting a CVE assigned and coordinating the release of the fix to the various Linux distributions.

Write a Security Policy.

(*^ – ^)ノ

Communication

- Work with the researcher

Communication

- Be involved in CVE process
- Create issues or bug reports for vulnerabilities
- Make announcements

Patching for Maintenance

- Clearly describes problem and solution

```
From 806d037671e133bd28a7864248763f643967973a Mon Sep 17 00:00:00 2001
From: Bram Moolenaar <Bram@vim.org>
Date: Tue, 25 Jan 2022 20:45:16 +0000
Subject: [PATCH] patch 8.2.4218: illegal memory access with bracketed paste in
 Ex mode

Problem:    Illegal memory access with bracketed paste in Ex mode.
Solution:   Reserve space for the trailing NUL.

--- a/src/edit.c
+++ b/src/edit.c
```

Patching for Maintenance

- Specific patch

```
--- a/src/edit.c
+++ b/src/edit.c
@@ -4440,7 +4440,8 @@ bracketed_paste(paste_mode_T mode, int d
                    break;

                case PASTE_EX:
-                   if (gap != NULL && ga_grow(gap, idx) == OK)
+                   // add one for the NUL that is going to be appended
+                   if (gap != NULL && ga_grow(gap, idx + 1) == OK)
                    {
                        mch_memmove((char *)gap->ga_data + gap->ga_len,
                                                          buf, (size_t)idx);
```

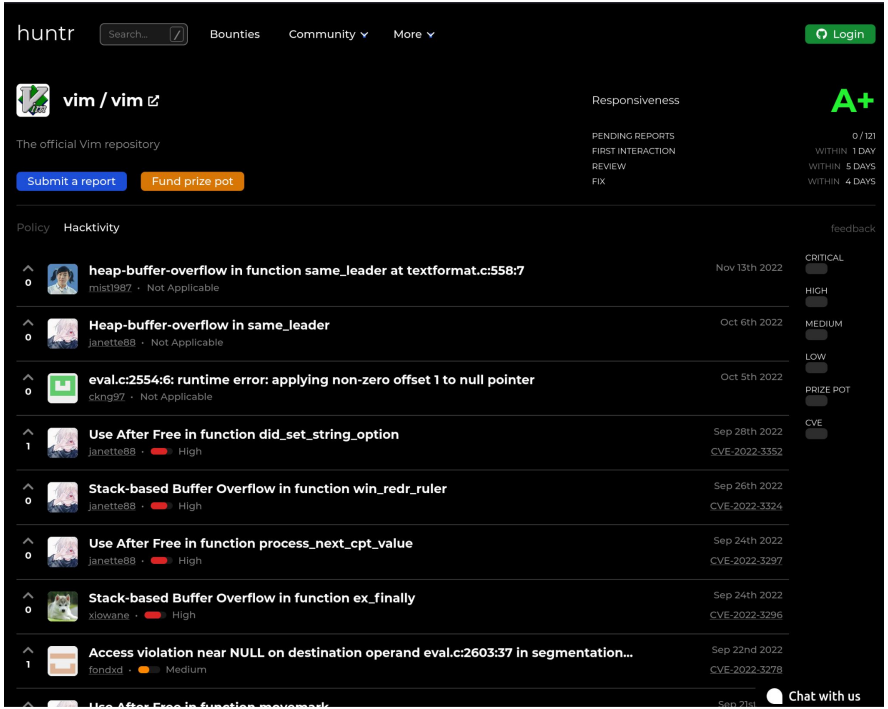
Patching for Maintenance

- Add test to reproduce vulnerability

```
--- a/src/testdir/test_paste.vim
+++ b/src/testdir/test_paste.vim
@@ -90,6 +90,9 @@ func Test_paste_ex_mode()
   unlet! foo
   call feedkeys("Qlet foo=\"\<Esc>[200~foo\<CR>bar\<Esc>[201~\"\<CR>vi\<CR>", 'xt')
   call assert_equal("foo\rbar", foo)
+
+  " pasting more than 40 bytes
+  exe "norm Q\<PasteStart>000000000000000000000000000000000000000000000000000000000000000000000000\<C-C>"
 endfunc

 func Test_paste_onechar()
```

Proactive discovery

- Static Analyzers
- Fuzzers
- Bug bounties



Getting Involved

- Automate or run static analyzers and fuzzers and projects
- Triage new reports
- Suggest a Security Policy

Recap

- It is okay to disclose vulnerabilities
- Write a Security Policy
- Communicate
- Patch for maintenance

Ubuntu Security Careers

Security Certifications Product Manager - CIS, FIPS, FedRAMP and more	Define Canonical security offerings from the kernel to the full spectrum of open source, along with compliance and audit mechanisms. Home based - EMEA
Security Engineer - Ubuntu	Combine your passion for programming, open source, Linux, and security to enhance the security of Ubuntu for millions of users. Home based - Worldwide
Ubuntu Security Manager	As an engineering manager at Canonical your primary responsibility is to the people you support: ensuring that they are growing as engineers, doing valuable work, and generally having a great time at Canonical. Home based - Worldwide

https://canonical.com/careers

Acknowledgement

Thanks to the entire Ubuntu Security Team for their input

Mauro Gaspari and Rex Tsai from Canonical for championing this talk

FIRST, the OpenFSS, and MITRE for taking my FOSS security questions

A **huge thank you to 한영빈(Youngbin Han)** and other UbuCon Asia 2022 organizers for their support

Thank you. Questions?

Resources

General:

OpenSSF's Concise Guides

OpenSSF's Preparing for Zero-Day (video)

FIRST

Common Weakness Enumeration (CWE)

LXD Security video

cveform.mitre.org

Proactive tooling lists:

Static Analyzers

Fuzzers

Glossary continued

- Backporting
- Bug
- Bug Bounty
- CNA

- CRD
- Coordinated Vulnerability Disclosure (CVD): a type of vulnerability disclosure where responsible parties are allowed time to address a vulnerability before public disclosure.

- CVE
- CVSS
- CWE
- Downstream
- Fuzzer
- Regression
- Security Policy
- Security Researcher
- Static Analyzer
- Upstream
- Vulnerability: a security flaw, glitch, or weakness found in software code the could be exploited by an attacked.