badkeys

Finding broken cryptographic keys

https://badkeys.info/

Hanno Böck

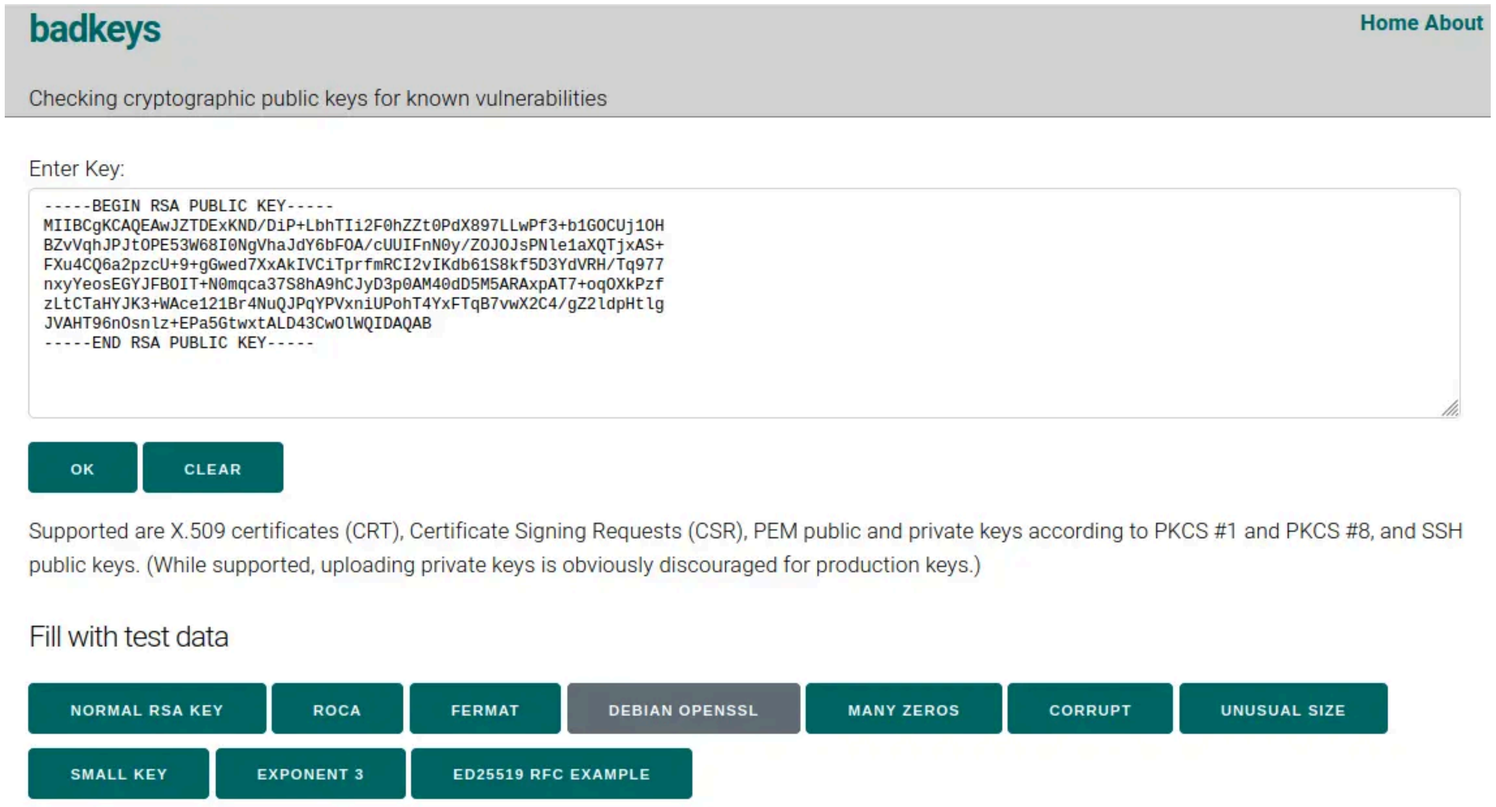
Security

GitHub security update: revoking weakly-generated SSH keys

On September 28, 2021, we received notice from the developer Axosoft regarding a vulnerability in a dependency of their popular git GUI client - GitKraken. An underlying issue with a dependency, called `keypair`, resulted in the GitKraken client generating weak SSH keys.

"There is no haveibeenpwned for public keys as far as I know"

user jornane on lobste.rs, 10/2021



badkeys.info

badkeys

A website, tool and library to check cryptographic keys for known vulnerabilities

Key Generation Vulnerabilities

- Shared prime factors
- Return of Coopersmith's attack / ROCA
- Fermat attack
- Debian OpenSSL Bug
- keypair / Gitkraken bug
- "Public Private Keys"

Debian OpenSSL Bug (CVE-2008-0166)

```
- --------------------------------------------------------------------------
Debian Security Advisory DSA-1571-1                  security@debian.org
http://www.debian.org/security/                           Florian Weimer
May 13, 2008                          http://www.debian.org/security/faq
- --------------------------------------------------------------------------

Package        : openssl
Vulnerability  : predictable random number generator
Problem type   : remote
Debian-specific: yes
CVE Id(s)      : CVE-2008-0166

Luciano Bello discovered that the random number generator in Debian's
openssl package is predictable.  This is caused by an incorrect
Debian-specific change to the openssl package (CVE-2008-0166).  As a
result, cryptographic key material may be guessable.
```

Keys depended on a limited number of factors like the PID and the architecture, limiting the number of possible keys to a few ten thousand

Old bugs never die

Matt Palmer Mar 7, 2020, 3:48:48 AM

to mozilla-dev-s...@lists.mozilla.org

(Pre) Certificate https://crt.sh/?id=2531502044 has been issued with a known weak key, specifically Debian weak key 2048/i386/rnd/pid17691. I believe this issuance to be in contravention of SSL.com's CPS, version 1.8, section 6.1.1.2, which states "SSL.com shall reject a certificate request if the request has a known weak Private Key".

- Matt

Matt Palmer on mozilla-dev-security-policy, 2020

Detecting the Debian OpenSSL bug

Existing tools and lists of affected keys were not exactly great

- Some of the old tools no longer worked on modern systems
- All collections of affected keys were incomplete
- Information about the exact details of the bug was confusing, incomplete, and sometimes wrong

Debian OpenSSL Bug variations

- PID (0 to 32767)
- OpenSSL and OpenSSH
- Different output if .rnd file exists
- Older and newer OpenSSL versions differ if the .rnd file does not exist
- Architectures: 32/64 bit, x86 vs. ppc/others vs. mips
- Key size
- RSA, DSA, Elliptic Curves (!)

https://github.com/badkeys/debianopenssl/

Earlier this year

"I should test DKIM keys with badkeys"

DKIM

TXT record at *key1._domainkey.hboeck.de*:

v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQE[...]

E-Mail header:

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=hboeck.de; s=key1; t=1715197611; bh=Z9fPSuWvmaUL/fgn9g0k2ORYPJe3Y3Vc5NiKvQJXc2w=; h=Date:From:To:Subject:Message-ID:MIME-Version:Content-Type: Content-Transfer-Encoding; b=TNyZHQd[...]

How to scan DKIM

Get lots of e-mails and extract selector/domain combinations

How to scan DKIM (better)

Try common selectors like dkim, mail, etc., with top domains

Scanning Tranco 1 Top Million list

Around 350,000 TXT records with a valid RSA key.

855 vulnerable to Debian OpenSSL bug (0.24%).

Domains with vulnerable keys

@cisco.com, @oracle.com, @skype.net, @github.partners,
@partner.crowdstrike.com, @partners.dropbox.com, @1password.com, @seznam.cz

Why?

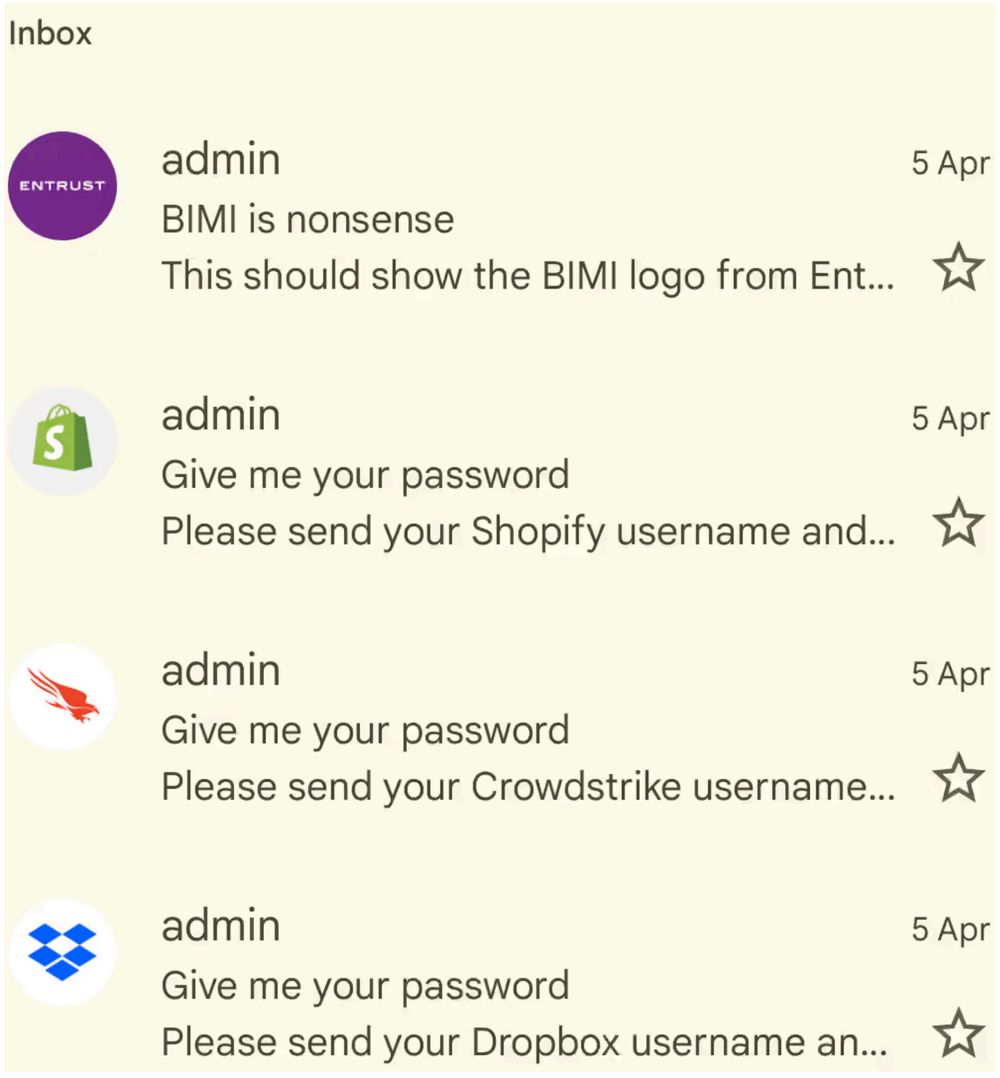
- 2006: Debian OpenSSL bug was introduced
- 2007: DKIM was published (RFC 4870)
- 2008: Debian OpenSSL bug was found

Most affected keys were configured as a CNAME to a host belonging to the company Cakemail

Trying to disclose a security issue to security@cakemail.com

We're writing to let you know that the group you tried to contact (security) may not exist, or you may not have permission to post messages to the group.

There were these logos...



More on DKIM findings and BIMI: Talk at MiniDebConf

https://16years.secvuln.info/

Fermat Attack

RSA

N = p * q

If you can calculate p, q from N, you can break RSA (factoring)

Fermat Factorization (1643)

Simple algorithm that can efficiently find prime factors if they are of similar size

How to not generate RSA keys

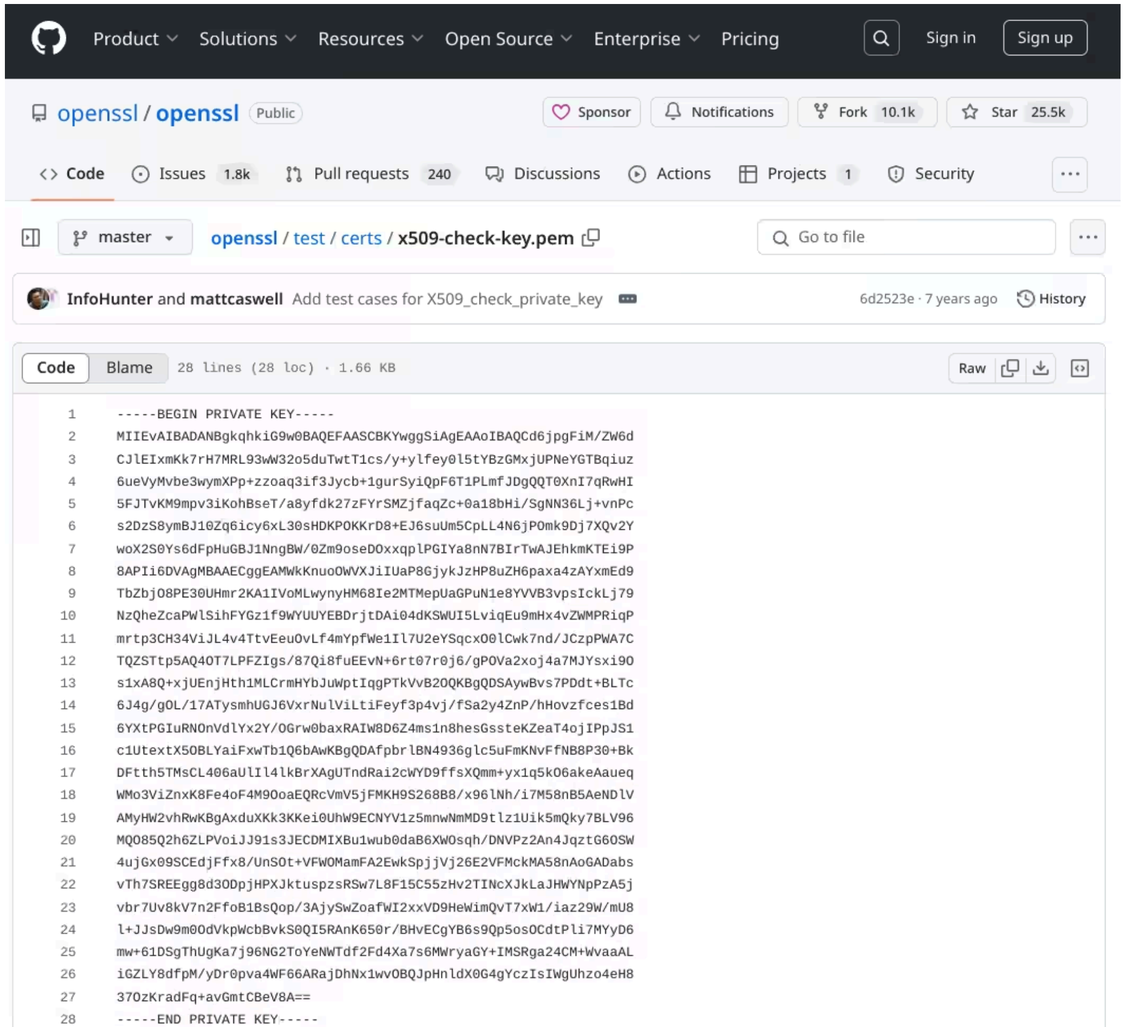
- Generate random number x
- Find next prime after x and use as p
- Find next prime after p and use as q

Are there such RSA keys?

Printers from Canon and Fujifilm generated keys breakable with Fermat Factorization (Safezone library from Rambus, CVE-2022-26320)

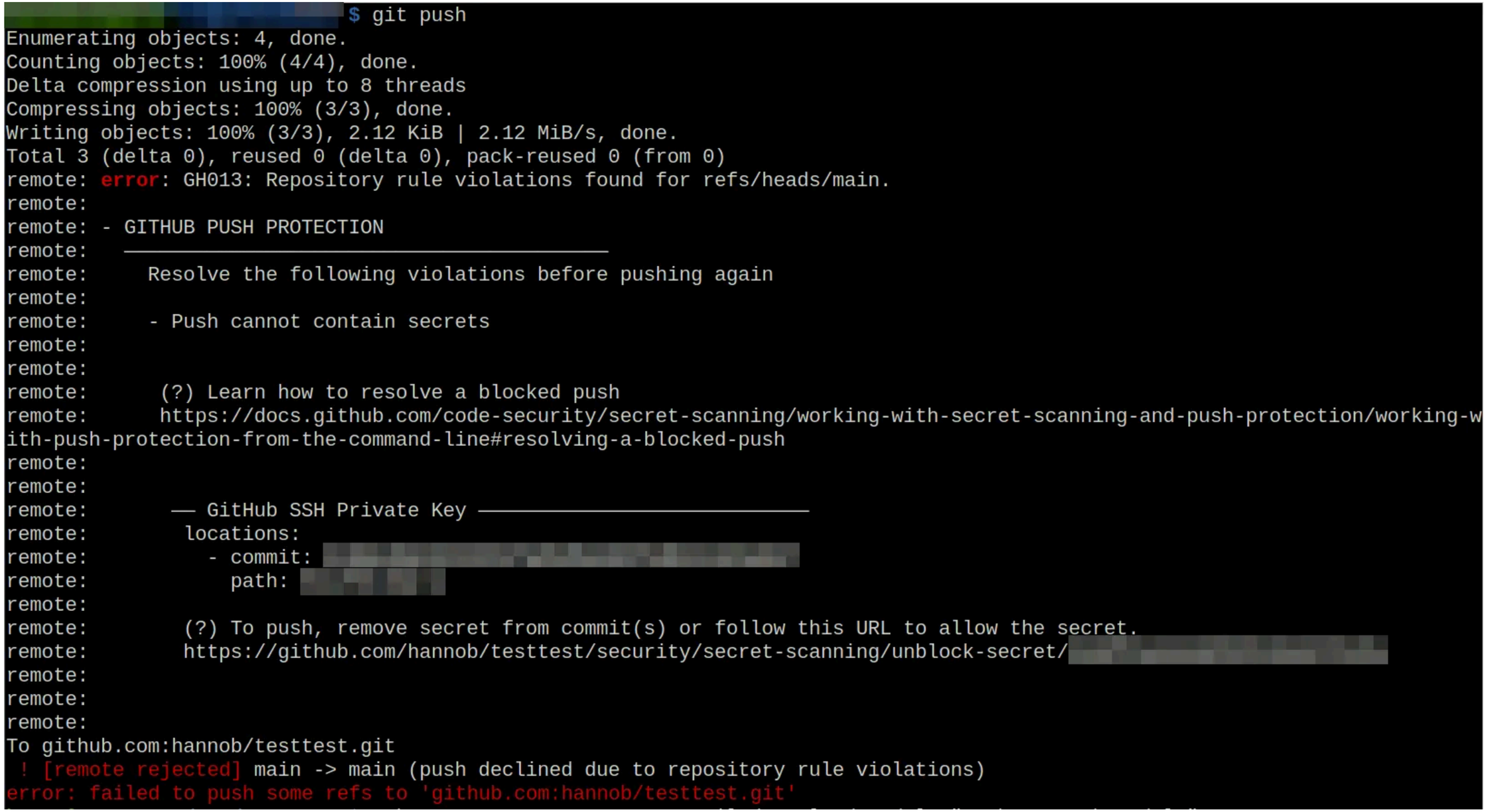
https://fermatattack.secvuln.info/

Public Private Keys



Many Public Private Keys

- Testcases in software
- Examples in documentation
- Hardcoded keys in software or firmware
- Leaks
- ...


$ git push
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 8 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 2.12 KiB | 2.12 MiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
remote: error: GH013: Repository rule violations found for refs/heads/main.
remote:
remote: - GITHUB PUSH PROTECTION
remote: ——————————————————————————————
remote: Resolve the following violations before pushing again
remote:
remote: - Push cannot contain secrets
remote:
remote:
remote: (?) Learn how to resolve a blocked push
remote: https://docs.github.com/code-security/secret-scanning/working-with-secret-scanning-and-push-protection/working-w
ith-push-protection-from-the-command-line#resolving-a-blocked-push
remote:
remote:
remote: —— GitHub SSH Private Key ——————————————————
remote: locations:
remote: - commit:
remote: path:
remote:
remote: (?) To push, remove secret from commit(s) or follow this URL to allow the secret.
remote: https://github.com/hannob/testtest/security/secret-scanning/unblock-secret/
remote:
remote:
remote:
To github.com:hannob/testtest.git
! [remote rejected] main -> main (push declined due to repository rule violations)
error: failed to push some refs to 'github.com:hannob/testtest.git'

Any recommendations how to deal with this?

(Github has no working security contact)

Plans for the Future of badkeys

Thanks to funding by NLnet/NGI0

Increase coverage of Public Private Keys

https://github.com/badkeys/keyfinder/

Monitoring

WebPKI, DNSSEC, DKIM

Key Compromise Service

You submit a compromised key, badkeys takes care of it

(Certificate Revocation, added to blocklist)

Call for help

Do you have any private keys you want to share with me?

Thanks for listening

Please use badkeys!

Questions?

https://badkeys.info