

# Vulnerability Discovery Results

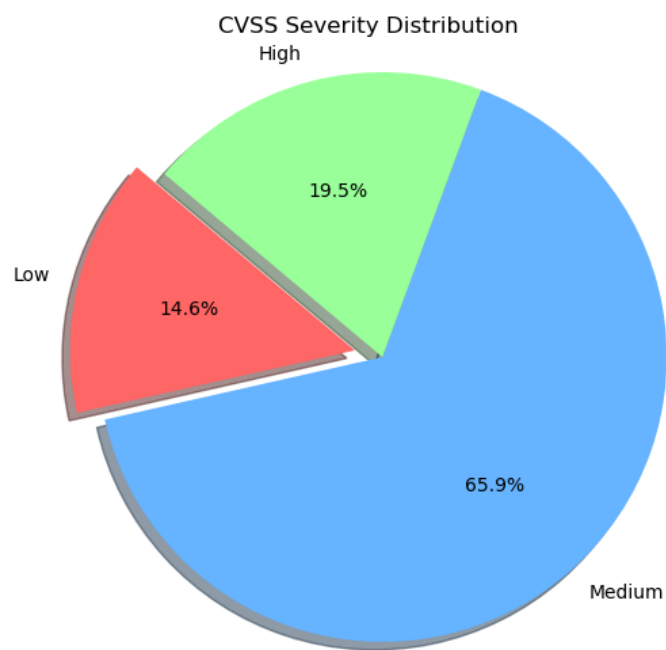
Friday 5<sup>th</sup> July, 2024

10:25

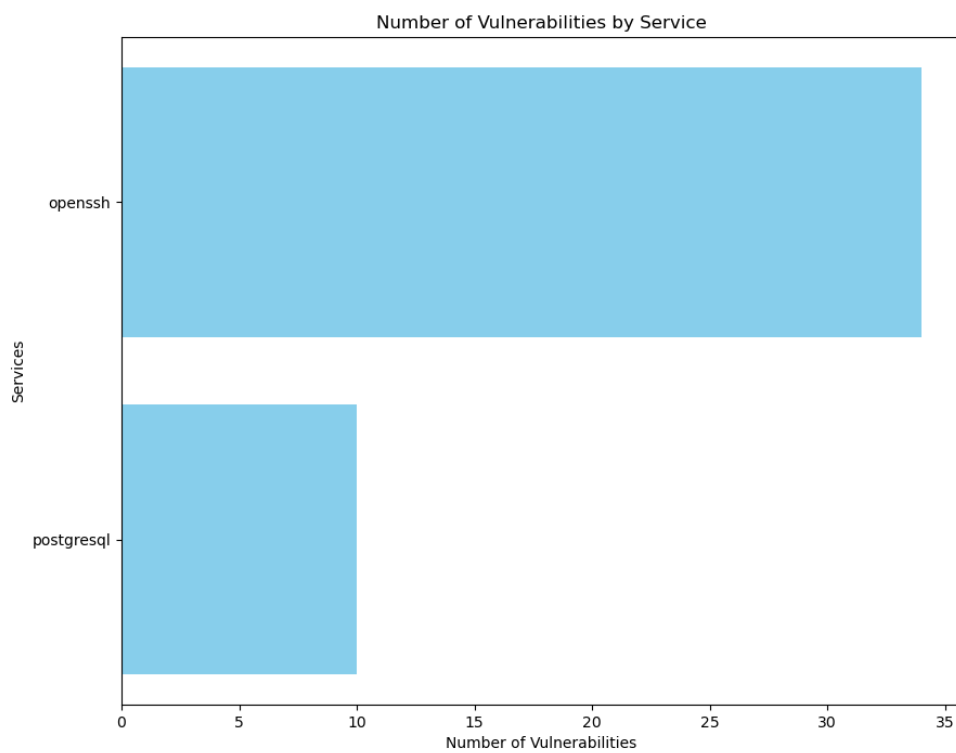
(UTC+2, PARIS)

Company Name	First Name	Last Name
Fedora	Terry	Quarrell

Name	OS Name	OS SP
metalin1	Linux	3.42.x



(a) Figure 1: Pie Chart



(b) Figure 2: Bar Chart

# Details

## 1.1 CVE-2015-5600

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The `kbdint_next_device` function in `auth2-chall.c` in `sshd` in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the `ssh -oKbdInteractiveDevices` option, as demonstrated by a modified client that provides a different password for each pam element on this list.

**CVSS: 8.5**

## 1.2 CVE-2016-6515

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The `auth_password` function in `auth-passwd.c` in `sshd` in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.

**CVSS: 7.8**

## 1.3 CVE-2014-1692

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The `hash_buffer` function in `schnorr.c` in OpenSSH through 6.4, when `Makefile.inc` is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.

**CVSS: 7.5**

## 1.4 CVE-2016-10009

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: Untrusted search path vulnerability in `ssh-agent.c` in `ssh-agent` in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.

**CVSS: 7.5**

## 1.5 CVE-2016-1908

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.

**CVSS: 7.5**

## 1.6 CVE-2015-8325

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The `do_setup_env` function in `session.c` in `sshd` in OpenSSH through 7.2p2, when the `UseLogin` feature is enabled and PAM is configured to read `.pam_environment` files in user home directories, allows local users to gain privileges by triggering a crafted environment for the `/bin/login` program, as demonstrated by an `LD_PRELOAD` environment variable.

**CVSS: 7.2**

## 1.7 CVE-2016-10012

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The shared memory manager (associated with pre-authentication compression) in `sshd` in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allow local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the `m_zback` and `m_zlib` data structures.

**CVSS: 7.2**

## 1.8 CVE-2015-6564

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: Use-after-free vulnerability in the `mm_answer_pam_free_ctx` function in `monitor.c` in `sshd` in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the `sshd` uid to send an unexpectedly early `MONITOR_REQ_PAM_FREE_CTX` request.

**CVSS: 6.9**

## 1.9 CVE-2016-10010

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: `sshd` in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to `serverloop.c`.

**CVSS: 6.9**

## 1.10 CVE-2020-15778

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: `scp` in OpenSSH through 8.3p1 allows command injection in the `scp.c` `toremove` function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of “anomalous argument transfers” because that could “stand a great chance of breaking existing workflows.”

**CVSS: 6.8**

### 1.11 CVE-2014-2532

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd\_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.

**CVSS: 5.8**

### 1.12 CVE-2014-2653

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The verify\_host\_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.

**CVSS: 5.8**

### 1.13 CVE-2019-6111

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized\_keys file).

**CVSS: 5.8**

### 1.14 CVE-2016-3115

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do\_authenticated1 and (2) session\_x11\_req functions.

**CVSS: 5.5**

### 1.15 CVE-2010-5107

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

**CVSS: 5.0**

### 1.16 CVE-2017-15906

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: The process\_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

**CVSS: 5.0**

### 1.17 CVE-2016-10708

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.

**CVSS: 5.0**

### 1.18 CVE-2018-15473

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

**CVSS: 5.0**

### 1.19 CVE-2018-15919

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states ‘We understand that the OpenSSH developers do not want to treat such a username enumeration (or “oracle”) as a vulnerability.’

**CVSS: 5.0**

### 1.20 CVE-2016-0778

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: The (1) roaming\_read and (2) roaming\_write functions in roaming\_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.

**CVSS: 4.6**

### 1.21 CVE-2015-5352

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: The x11\_open\_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline

for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.

**CVSS: 4.3**

## 1.22 CVE-2016-6210

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.

**CVSS: 4.3**

## 1.23 CVE-2020-14145

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

**CVSS: 4.3**

## 1.24 CVE-2016-20012

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

**CVSS: 4.3**

## 1.25 CVE-2016-0777

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: The `resend_bytes` function in `roaming_common.c` in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

**CVSS: 4.0**

## 1.26 CVE-2019-6109

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::~::~\*

Summary: An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control

codes to hide additional files being transferred. This affects `refresh_progress_meter()` in `progressmeter.c`.

**CVSS: 4.0**

## 1.27 CVE-2019-6110

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

**CVSS: 4.0**

## 1.28 CVE-2018-20685

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: In OpenSSH 7.9, `scp.c` in the `scp` client allows remote SSH servers to bypass intended access restrictions via the filename of `.` or an empty filename. The impact is modifying the permissions of the target directory on the client side.

**CVSS: 2.6**

## 1.29 CVE-2021-36368

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without `-oLogLevel=verbose`, and an attacker has silently modified the server to support the `None` authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed."

**CVSS: 2.6**

## 1.30 CVE-2016-10011

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: `authfile.c` in `sshd` in OpenSSH before 7.4 does not properly consider the effects of `realloc` on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.

**CVSS: 2.1**

## 1.31 CVE-2015-6563

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The monitor component in `sshd` in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in `MONITOR_REQ_PAM_INIT_CTX` requests, which allows local users to conduct impersonation attacks by leveraging any



SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR\_REQ\_PWNAM request, related to monitor.c and monitor\_wrap.c.

**CVSS: 1.9**

### 1.32 CVE-2023-38408

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

**CVSS: N/A**

### 1.33 CVE-2023-48795

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGO before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

**CVSS: N/A**

### 1.34 CVE-2023-51385

!-> CVE for cpe:2.3:a:openbsd:openssh:6.1:::.\*

Summary: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an

expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

**CVSS: N/A**

### **1.35 CVE-2019-10211**

!-> CVE for cpe:2.3:a:postgresql:postgresql:9.2.24:::\*

Summary: PostgreSQL Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via bundled OpenSSL executing code from unprotected directory.

**CVSS: 7.5**

### **1.36 CVE-2017-14798**

!-> CVE for cpe:2.3:a:postgresql:postgresql:9.2.24:::\*

Summary: A race condition in the postgresql init script could be used by attackers able to access the postgresql account to escalate their privileges to root.

**CVSS: 6.9**

### **1.37 CVE-2020-25694**

!-> CVE for cpe:2.3:a:postgresql:postgresql:9.2.24:::\*

Summary: A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If a client application that creates additional database connections only reuses the basic connection parameters while dropping security-relevant parameters, an opportunity for a man-in-the-middle attack, or the ability to observe clear-text transmissions, could exist. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

**CVSS: 6.8**

### **1.38 CVE-2020-25695**

!-> CVE for cpe:2.3:a:postgresql:postgresql:9.2.24:::\*

Summary: A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. An attacker having permission to create non-temporary objects in at least one schema can execute arbitrary SQL functions under the identity of a superuser. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

**CVSS: 6.5**

### **1.39 CVE-2018-1115**

!-> CVE for cpe:2.3:a:postgresql:postgresql:9.2.24:::\*

Summary: postgresql before versions 10.4, 9.6.9 is vulnerable in the adminpack extension, the pg\_catalog.pg\_logfile\_rotate() function doesn't follow the same ACLs than pg\_rotate\_logfile. If the adminpack is added to a database, an attacker able to connect to it could exploit this to force log rotation.

**CVSS: 6.4**

#### 1.40 CVE-2021-23214

!-> CVE for cpe:2.3:a:postgresql:postgresql:9.2.24:::\*

Summary: When the server is configured to use trust authentication with a clientcert requirement or to use cert authentication, a man-in-the-middle attacker can inject arbitrary SQL queries when a connection is first established, despite the use of SSL certificate verification and encryption.

**CVSS: 5.1**

#### 1.41 CVE-2019-10127

!-> CVE for cpe:2.3:a:postgresql:postgresql:9.2.24:::\*

Summary: A vulnerability was found in postgresql versions 11.x prior to 11.3. The Windows installer for BigSQL-supplied PostgreSQL does not lock down the ACL of the binary installation directory or the ACL of the data directory; it keeps the inherited ACL. In the default configuration, an attacker having both an unprivileged Windows account and an unprivileged PostgreSQL account can cause the PostgreSQL service account to execute arbitrary code. An attacker having only the unprivileged Windows account can read arbitrary data directory files, essentially bypassing database-imposed read access limitations. An attacker having only the unprivileged Windows account can also delete certain data directory files.

**CVSS: 4.3**

#### 1.42 CVE-2019-10128

!-> CVE for cpe:2.3:a:postgresql:postgresql:9.2.24:::\*

Summary: A vulnerability was found in postgresql versions 11.x prior to 11.3. The Windows installer for EnterpriseDB-supplied PostgreSQL does not lock down the ACL of the binary installation directory or the ACL of the data directory; it keeps the inherited ACL. In the default configuration, this allows a local attacker to read arbitrary data directory files, essentially bypassing database-imposed read access limitations. In plausible non-default configurations, an attacker having both an unprivileged Windows account and an unprivileged PostgreSQL account can cause the PostgreSQL service account to execute arbitrary code.

**CVSS: 4.1**

#### 1.43 CVE-2021-3393

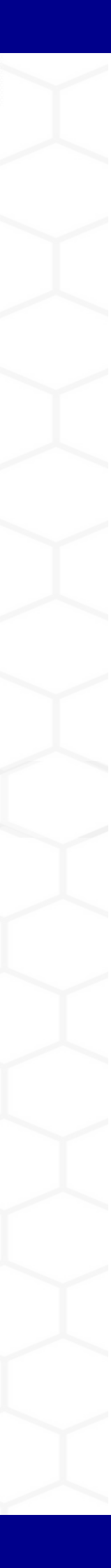
!-> CVE for cpe:2.3:a:postgresql:postgresql:9.2.24:::\*

Summary: An information leak was discovered in postgresql in versions before 13.2, before 12.6 and before 11.11. A user having UPDATE permission but not SELECT permission to a particular column could craft queries which, under some circumstances, might disclose values from that column in error messages. An attacker could use this flaw to obtain information stored in a column they are allowed to write but not read.

**CVSS: 3.5**

#### 1.44 CVE-2019-10210

!-> CVE for cpe:2.3:a:postgresql:postgresql:9.2.24:::\*



Summary: Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via superuser writing password to unprotected temporary file.

**CVSS: 1.9**