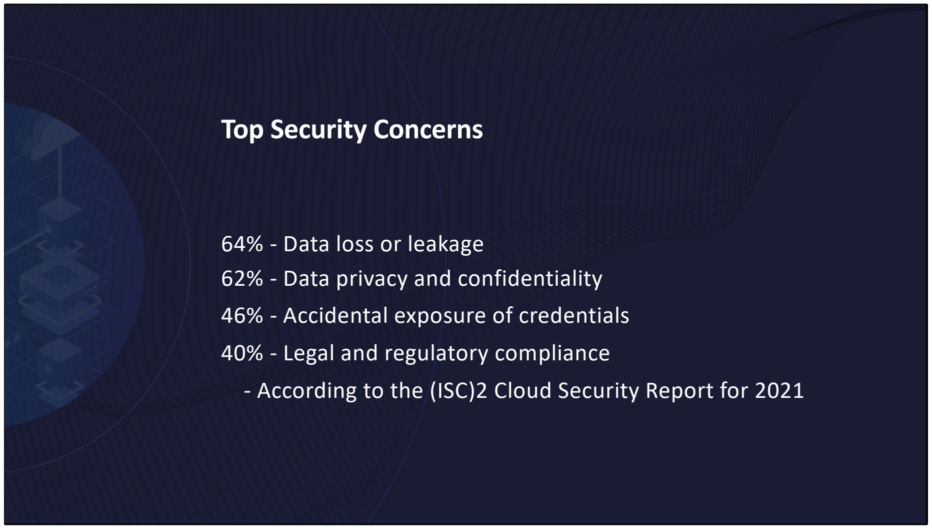
Central Canada

Db2 Users Group

Decoding Db2 Security Bulletins

Mitchell Waite, IBM

September 19, 2023



Top Security Concerns

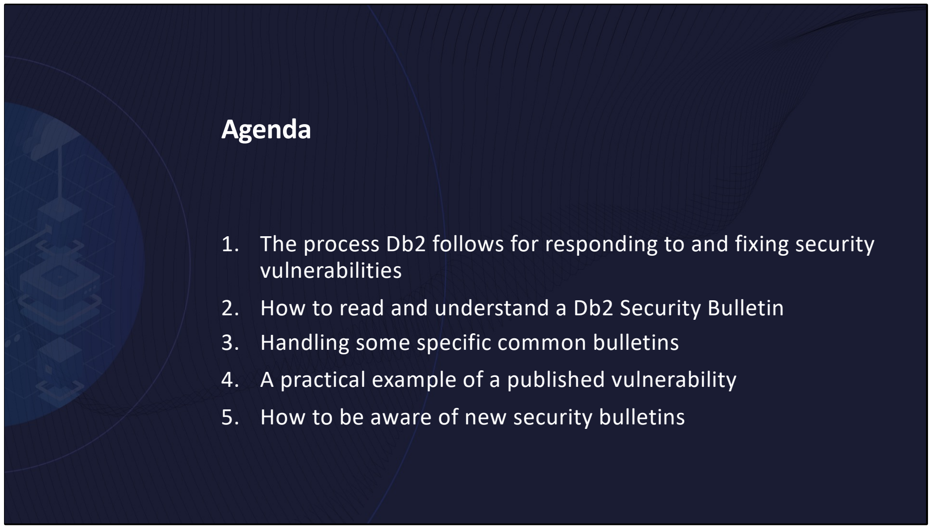
64% - Data loss or leakage

62% - Data privacy and confidentiality

46% - Accidental exposure of credentials

40% - Legal and regulatory compliance

- According to the (ISC)2 Cloud Security Report for 2021



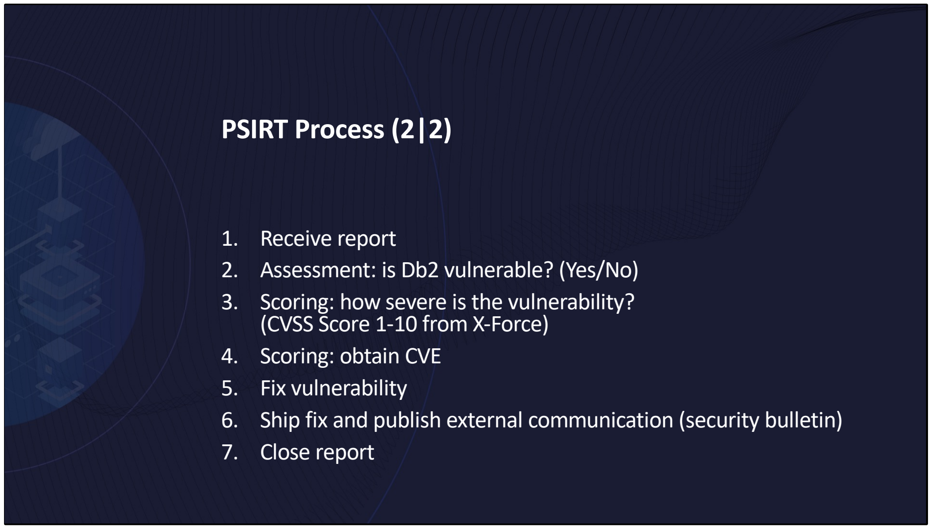
Agenda

1. The process Db2 follows for responding to and fixing security vulnerabilities
2. How to read and understand a Db2 Security Bulletin
3. Handling some specific common bulletins
4. A practical example of a published vulnerability
5. How to be aware of new security bulletins

PSIRT Process (1|2)

- Product Security Incident Response Team (PSIRT) deals with reported vulnerabilities
- Website: https://www.ibm.com/trust/security-psirt

Disclaimer: this process is how we currently operate, not a commitment for the rest of time.



PSIRT Process (2|2)

1. Receive report
2. Assessment: is Db2 vulnerable? (Yes/No)
3. Scoring: how severe is the vulnerability?
   (CVSS Score 1-10 from X-Force)
4. Scoring: obtain CVE
5. Fix vulnerability
6. Ship fix and publish external communication (security bulletin)
7. Close report

- First, a report of a vulnerability in Db2 is received by IBM. Reports can be received by IBM directly or through HackerOne. HackerOne is a community of individuals known as “ethical hackers” that receive points for successful reports. (https://www.hackerone.com/)

- Once a report is received,

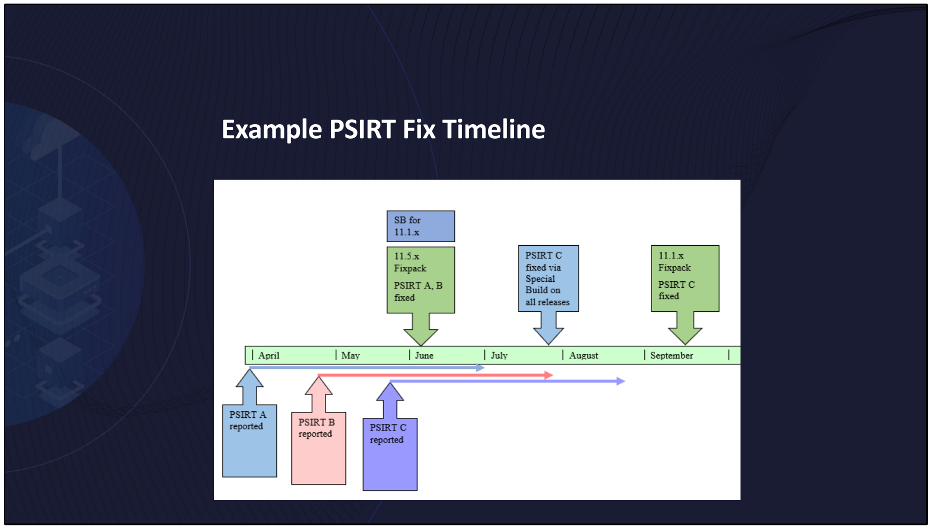
- If Db2 is assessed as being vulnerable, the vulnerability is scored by IBM X-Force
IBM Db2 does not score vulnerabilities, IBM X-Force does (https://exchange.xforce.ibmcloud.com/)

- Once the vulnerability is scored, A CVE number is assigned. The CVE number will remain in “reserved” state in the NVD until a fix is published.
CVE stands for Common Vulnerabilities and Exposures.
CVEs are reserved from MITRE (https://cve.mitre.org/index.html), a part of NVD (U.S. National Vulnerability Database).
CVE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)

- Developers of the appropriate Db2 component fix the vulnerability. The timeline depends on the severity of the vulnerability.

- Fix is shipped as part of a security special build, and external communications are published. This includes the Security Bulletin and Known Issue. The CVE details are also made public and the NVD is updated.

- Last step is to close the PSIRT report



Example PSIRT Fix Timeline

This is an example timeline of what a PSIRT fix schedule might look like.

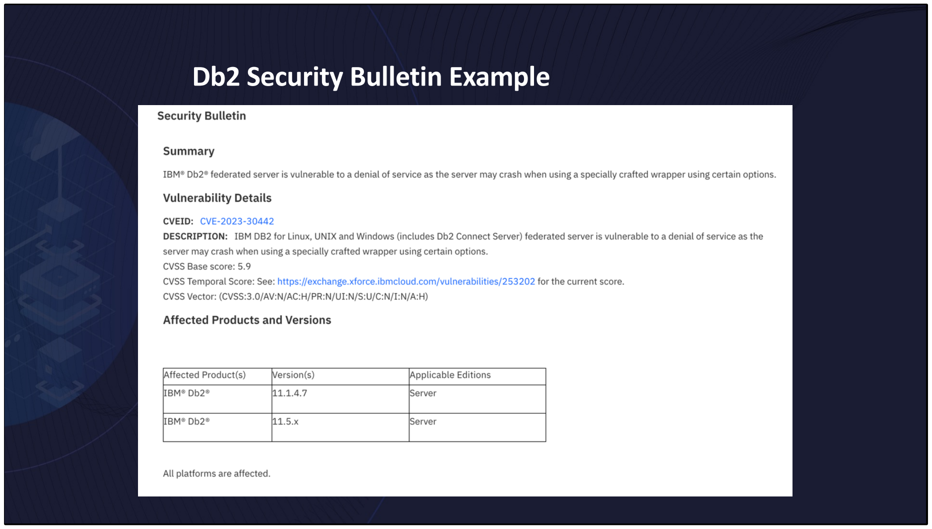
Assume PSIRT A is reported at the beginning of April, PSIRT B is reported at the beginning of May, and PSIRT C is reported at the beginning of June. For the purposes of this example, there is an 11.5 fix pack scheduled in the first week of June and an 11.1 fix pack scheduled mid-way through September.

In this timeline, a fix was developed for both PSIRT A and PSIRT in time for the 11.5 fix pack. This means that the fix will be shipped as part of an official 11.5 fix pack, and at the same time a special build for 11.1 will be released to fix the PSIRT on downlevel releases.

PSIRT C was reported later, but the fix deadline is before the next 11.1 fix pack, so it will be fixed at the end of July using a security special build on all releases. The 11.1 fix pack in September, and the next 11.5 fix pack after that will be the official Db2 releases containing a fix for PSIRT C.

Secure engineering at IBM: https://www.ibm.com/trust/security-spbd

2. Reading and understanding security bulletins



Db2 Security Bulletin Example

Security Bulletin

Summary

IBM® Db2® federated server is vulnerable to a denial of service as the server may crash when using a specially crafted wrapper using certain options.

Vulnerability Details

CVEID: CVE-2023-30442
DESCRIPTION: IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) federated server is vulnerable to a denial of service as the server may crash when using a specially crafted wrapper using certain options.
CVSS Base score: 5.9
CVSS Temporal Score: See: https://exchange.xforce.ibmcloud.com/vulnerabilities/253202 for the current score.
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

Affected Products and Versions

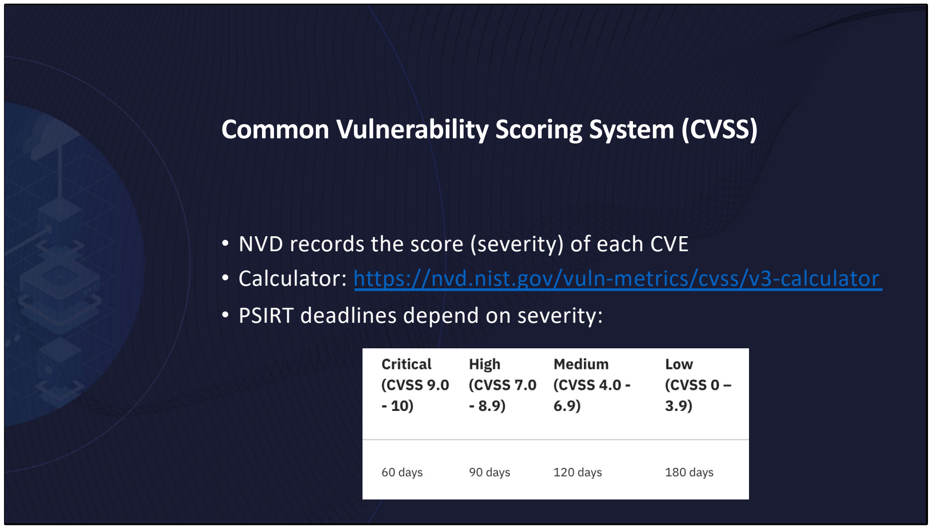
Affected Product(s)	Version(s)	Applicable Editions
IBM® Db2®	11.1.4.7	Server
IBM® Db2®	11.5.x	Server

All platforms are affected.

This is an example of what a recent security security bulletin looks like. It captures a summary, the vulnerability description, the CVSS score and vector, and a chart of impacted products and versions.

The chart will indicate which releases of Db2 are affected, and whether the client, server, or both are affected. In this case the 11.1 and 11.5 servers are affected.

Note: If you find the description is very general and seems to apply to everyone, it is because it does apply and everyone should apply the fix. IBM does not disclose key Db2 functionality nor replication steps for a vulnerability to avoid providing too much information to any potential malicious attacker. IBM does not want to enable a malicious attacker with sufficient knowledge to craft an exploit of the vulnerability.



Common Vulnerability Scoring System (CVSS)

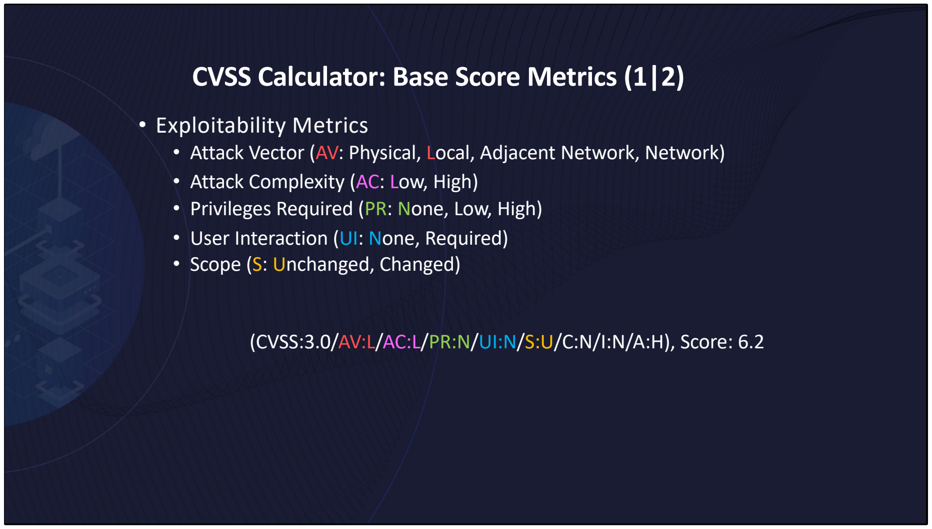
- NVD records the score (severity) of each CVE
- Calculator: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- PSIRT deadlines depend on severity:

Critical (CVSS 9.0 - 10)	**High (CVSS 7.0 - 8.9)**	**Medium (CVSS 4.0 - 6.9)**	**Low (CVSS 0 – 3.9)**
60 days	90 days	120 days	180 days

CVSS is a system for rating the severity of vulnerabilities.

CVEs are assigned a score that indicates the severity of a vulnerability. For Db2, we use CVSS 3.0 scores. NVD publishes a calculator that can be used to determine

Within IBM, deadlines for publishing a fix depends on the severity of the vulnerability. In extenuating circumstances, such as the Log4J vulnerability, PSIRT deadlines may be shorter.



CVSS Calculator: Base Score Metrics (1|2)

- Exploitability Metrics
  - Attack Vector (AV: Physical, Local, Adjacent Network, Network)
  - Attack Complexity (AC: Low, High)
  - Privileges Required (PR: None, Low, High)
  - User Interaction (UI: None, Required)
  - Scope (S: Unchanged, Changed)

(CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H), Score: 6.2

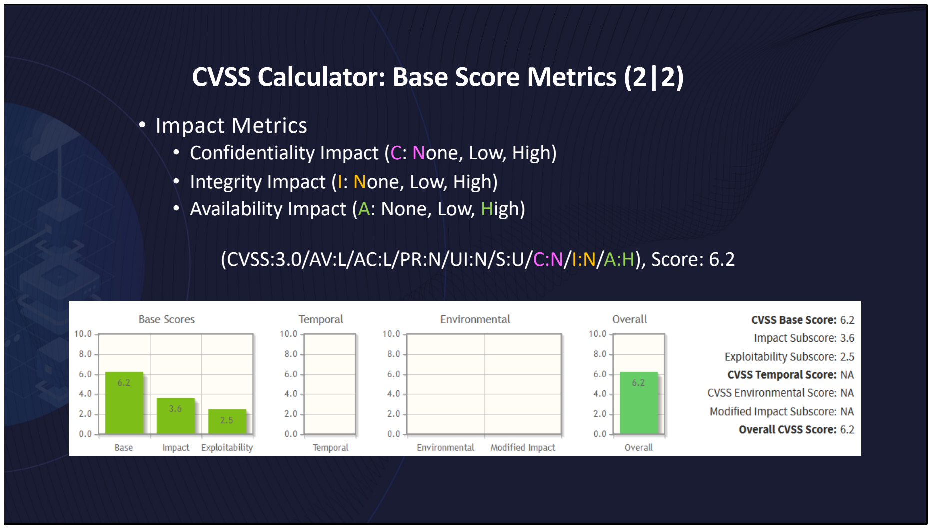
The CVSS score is based on 5 exploitability metrics, 5 exploitability metrics and 3 impact metrics.

CVSS Calculator 3.0: https://www.first.org/cvss/calculator/3.0
CVSS Specification document: https://www.first.org/cvss/v3.0/specification-document

Exploitability metrics describe the vulnerability itself, such as the complexity and where the vulnerability can be exploited.

The 5 metrics are:
- Attack vector (context in which the vulnerability can be exploited)
- Attack Complexity (complexity of conditions that must exist for the vulnerability to be exploited)
- Privileges required (what privileges an attacker requires to be able to exploit)
- User Interaction (whether any user interaction is required to exploit)
- Scope (Whether the vulnerability affects components beyond the affected component’s security scope)

Adjacent Network can be a trusted network, VPN, etc.
Example: A "local" attacker means the malicious user needs access to the Db2 server’s operating system and can log into the server. That means it is not vulnerable through SQL.



CVSS Calculator: Base Score Metrics (2|2)

- Impact Metrics
  - Confidentiality Impact (C: None, Low, High)
  - Integrity Impact (I: None, Low, High)
  - Availability Impact (A: None, Low, High)

(CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H), Score: 6.2

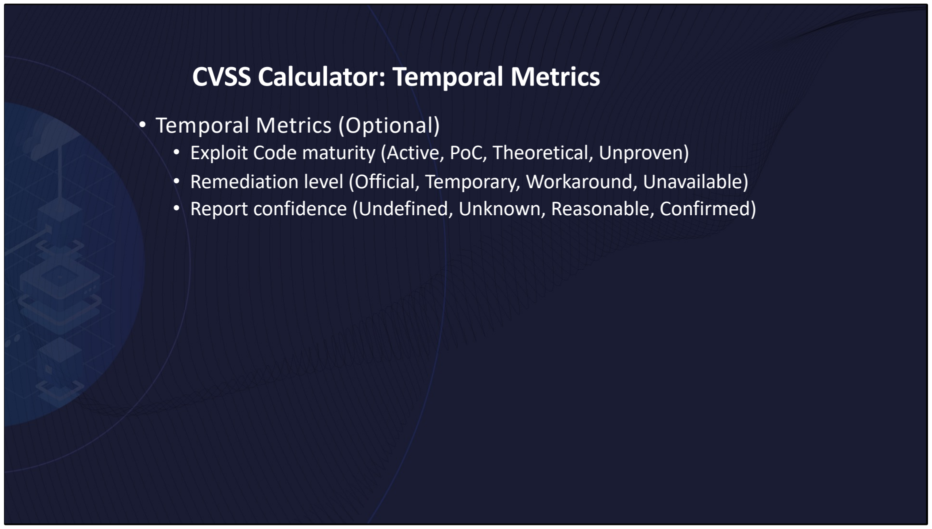
CVSS Base Score: 6.2
Impact Subscore: 3.6
Exploitability Subscore: 2.5
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 6.2

Impact metrics indicate the effects of a successful exploit. Impact metrics are the following:

- Confitdentiality (measures the confidentially of managed information)
- Integrity (measures the trustworthiness of managed information)
- Availability (measures the impact to the availability of the impacted system)

The Impact could in theory be to all three metrics (Confidentiality, Integrity, Availability) at once.

Base Score is made up of Exploitability and Impact metrics.
All base metrics are required to generate a base score.



CVSS Calculator: Temporal Metrics

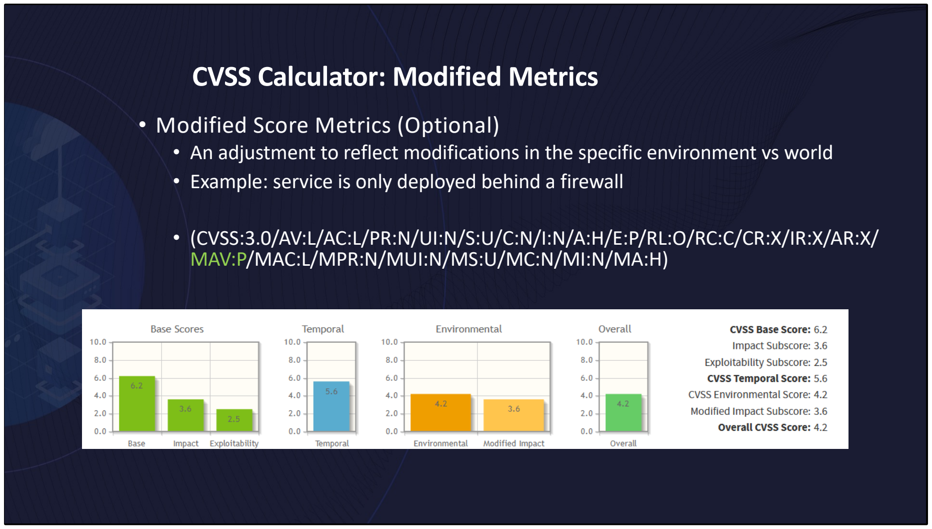
- Temporal Metrics (Optional)
  - Exploit Code maturity (Active, PoC, Theoretical, Unproven)
  - Remediation level (Official, Temporary, Workaround, Unavailable)
  - Report confidence (Undefined, Unknown, Reasonable, Confirmed)

In addition to the base score, IBM X-Force publishes a temporal score.

The temporal CVSS score is an adjustment to represent the current exploitability and the availability of fixes.

- Exploit Code Maturity (whether any code exists that can exploit the vulnerability in question)
- Remediation Level (whether a fix or workaround is available from the vendor)
- Report confidence (measures the confidence that a vulnerability report is legitimate)

As an example, the “Report confidence” for vulnerabilities listed on Db2’s “Published Security Vulnerabilities” page is ”Confirmed”, as the vulnerabilities have been acknowledged by IBM.



CVSS Calculator: Modified Metrics

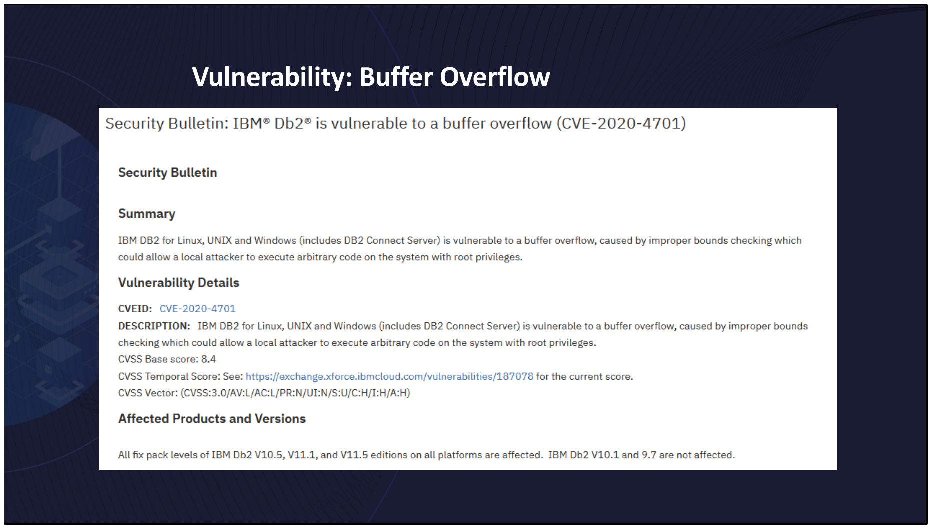
- Modified Score Metrics (Optional)
  - An adjustment to reflect modifications in the specific environment vs world
  - Example: service is only deployed behind a firewall

  - (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C/CR:X/IR:X/AR:X/ MAV:P/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:N/MA:H)

CVSS Base Score: 6.2
Impact Subscore: 3.6
Exploitability Subscore: 2.5
CVSS Temporal Score: 5.6
CVSS Environmental Score: 4.2
Modified Impact Subscore: 3.6
Overall CVSS Score: 4.2

IBM does not use modified score metrics, since we are scoring for all customers.
MAV: P stands or Modified Attack Vector: Physical

3. Handling some specific common bulletins



Vulnerability: Buffer Overflow

Security Bulletin: IBM® Db2® is vulnerable to a buffer overflow (CVE-2020-4701)

Security Bulletin

Summary

IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges.

Vulnerability Details

CVEID: CVE-2020-4701
DESCRIPTION: IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges.
CVSS Base score: 8.4
CVSS Temporal Score: See: https://exchange.xforce.ibmcloud.com/vulnerabilities/187078 for the current score.
CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

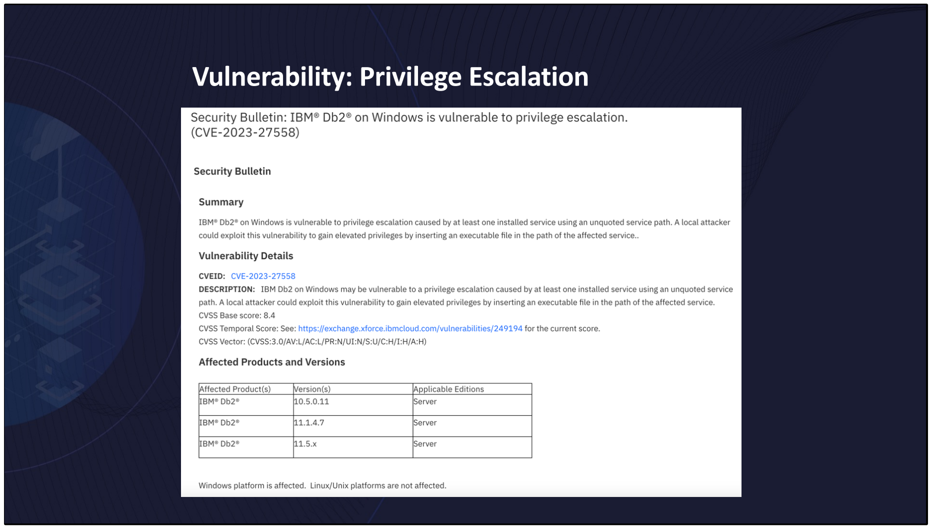
Affected Products and Versions

All fix pack levels of IBM Db2 V10.5, V11.1, and V11.5 editions on all platforms are affected. IBM Db2 V10.1 and 9.7 are not affected.

Buffer overflow: a command that overflows a buffer (corrupting memory adjacent to the buffer) and can theoretically lead to an arbitrary code execution and/or privilege escalation.

OWASP Top 10: https://owasp.org/www-project-top-ten/
Buffer Overflow: https://owasp.org/www-community/vulnerabilities/Buffer_Overflow

https://www.ibm.com/support/pages/node/6370025



Vulnerability: Privilege Escalation

Security Bulletin: IBM® Db2® on Windows is vulnerable to privilege escalation. (CVE-2023-27558)

Security Bulletin

Summary

IBM® Db2® on Windows is vulnerable to privilege escalation caused by at least one installed service using an unquoted service path. A local attacker could exploit this vulnerability to gain elevated privileges by inserting an executable file in the path of the affected service..

Vulnerability Details

CVEID: CVE-2023-27558
DESCRIPTION: IBM Db2 on Windows may be vulnerable to a privilege escalation caused by at least one installed service using an unquoted service path. A local attacker could exploit this vulnerability to gain elevated privileges by inserting an executable file in the path of the affected service.
CVSS Base score: 8.4
CVSS Temporal Score: See: https://exchange.xforce.ibmcloud.com/vulnerabilities/249194 for the current score.
CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

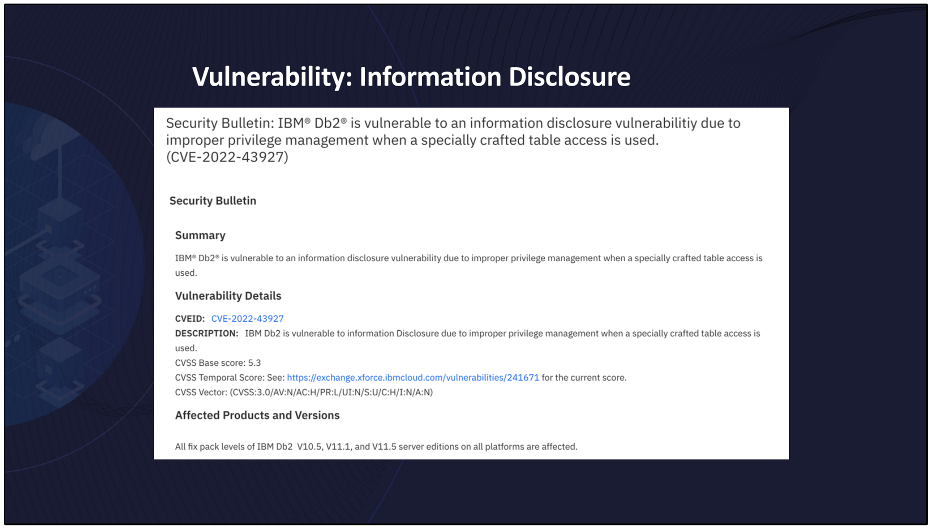
Affected Products and Versions

Affected Product(s)	Version(s)	Applicable Editions
IBM® Db2®	10.5.0.11	Server
IBM® Db2®	11.1.4.7	Server
IBM® Db2®	11.5.x	Server

Windows platform is affected. Linux/Unix platforms are not affected.

Privilege escalation: an exploit where a user can gain privileges above what was assigned. Impact of a privilege escalation can vary depending on the context.

https://www.ibm.com/support/pages/node/7010571



Vulnerability: Information Disclosure

Security Bulletin: IBM® Db2® is vulnerable to an information disclosure vulnerabilitiy due to improper privilege management when a specially crafted table access is used. (CVE-2022-43927)

Security Bulletin

Summary

IBM® Db2® is vulnerable to an information disclosure vulnerability due to improper privilege management when a specially crafted table access is used.

Vulnerability Details

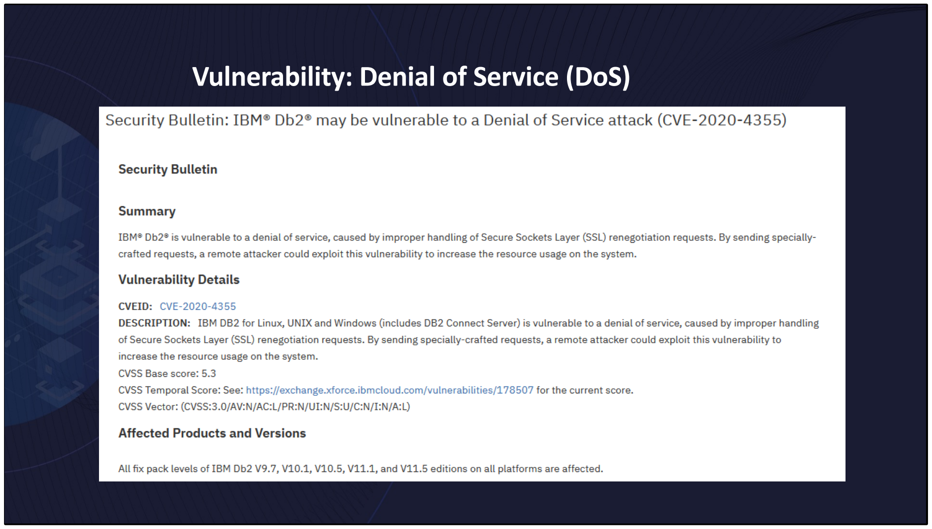
CVEID: CVE-2022-43927
DESCRIPTION: IBM Db2 is vulnerable to information Disclosure due to improper privilege management when a specially crafted table access is used.
CVSS Base score: 5.3
CVSS Temporal Score: See: https://exchange.xforce.ibmcloud.com/vulnerabilities/241671 for the current score.
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

Affected Products and Versions

All fix pack levels of IBM Db2 V10.5, V11.1, and V11.5 server editions on all platforms are affected.

Information disclosure occurs when the vulnerability reveals sensitive information that the attacker does not normally have the privilege to access.

https://www.ibm.com/support/pages/node/6953759



Vulnerability: Denial of Service (DoS)

Security Bulletin: IBM® Db2® may be vulnerable to a Denial of Service attack (CVE-2020-4355)

Security Bulletin

Summary

IBM® Db2® is vulnerable to a denial of service, caused by improper handling of Secure Sockets Layer (SSL) renegotiation requests. By sending specially-crafted requests, a remote attacker could exploit this vulnerability to increase the resource usage on the system.

Vulnerability Details

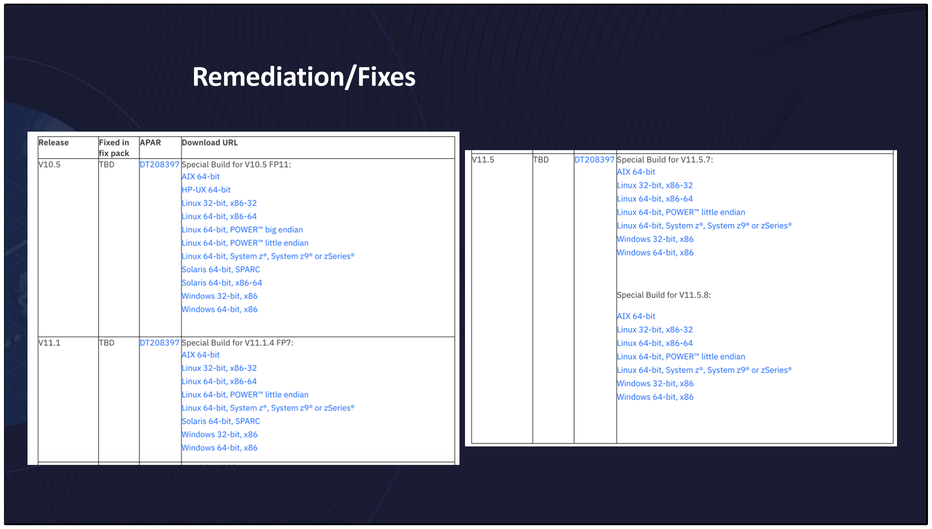
CVEID: CVE-2020-4355
DESCRIPTION: IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) is vulnerable to a denial of service, caused by improper handling of Secure Sockets Layer (SSL) renegotiation requests. By sending specially-crafted requests, a remote attacker could exploit this vulnerability to increase the resource usage on the system.
CVSS Base score: 5.3
CVSS Temporal Score: See: https://exchange.xforce.ibmcloud.com/vulnerabilities/178507 for the current score.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Affected Products and Versions

All fix pack levels of IBM Db2 V9.7, V10.1, V10.5, V11.1, and V11.5 editions on all platforms are affected.

A denial of service occurs when an attacker uses the vulnerability to prevent legitimate usage of Db2. This could mean consuming system resources or causing a database crash.

https://www.ibm.com/support/pages/node/6242350



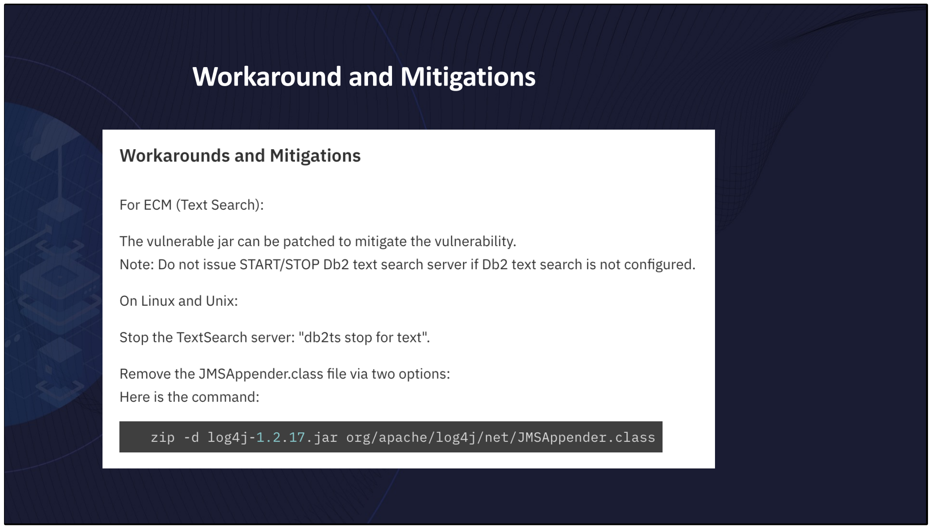
Remediation/Fixes

Release	Fixed in fix pack	APAR	Download URL
V10.5	TBD	DT208397	Special Build for V10.5 FP11: AIX 64-bit HP-UX 64-bit Linux 32-bit, x86-32 Linux 64-bit, x86-64 Linux 64-bit, POWER™ big endian Linux 64-bit, POWER™ little endian Linux 64-bit, System z®, System z9® or zSeries® Solaris 64-bit, SPARC Solaris 64-bit, x86-64 Windows 32-bit, x86 Windows 64-bit, x86
V11.1	TBD	DT208397	Special Build for V11.1.4 FP7: AIX 64-bit Linux 32-bit, x86-32 Linux 64-bit, x86-64 Linux 64-bit, POWER™ little endian Linux 64-bit, System z®, System z9® or zSeries® Solaris 64-bit, SPARC Windows 32-bit, x86 Windows 64-bit, x86
V11.5	TBD	DT208397	Special Build for V11.5.7: AIX 64-bit Linux 32-bit, x86-32 Linux 64-bit, x86-64 Linux 64-bit, POWER™ little endian Linux 64-bit, System z®, System z9® or zSeries® Windows 32-bit, x86 Windows 64-bit, x86 Special Build for V11.5.8: AIX 64-bit Linux 32-bit, x86-32 Linux 64-bit, x86-64 Linux 64-bit, POWER™ little endian Linux 64-bit, System z®, System z9® or zSeries® Windows 32-bit, x86 Windows 64-bit, x86

For a given vulnerability, special builds will be provided for all affected platforms.

On 10.5 and 11.1, security fixes are delivered in a “Security Special Build” stream that only includes security fixes.

For 11.5.x releases, security fixes are delivered as part of the “Continuous Special Build” stream that includes both security and APAR fixes. Continuous special builds are produced on the latest 11.5 release and one prior. As of the time of this presentation, that means security fixes are provided on 11.5.8 and 11.5.7. For most platforms, the universal_fixpack images are provided, which can update all installation types.



Workaround and Mitigations

Workarounds and Mitigations

For ECM (Text Search):

The vulnerable jar can be patched to mitigate the vulnerability.
Note: Do not issue START/STOP Db2 text search server if Db2 text search is not configured.

On Linux and Unix:

Stop the TextSearch server: "db2ts stop for text".

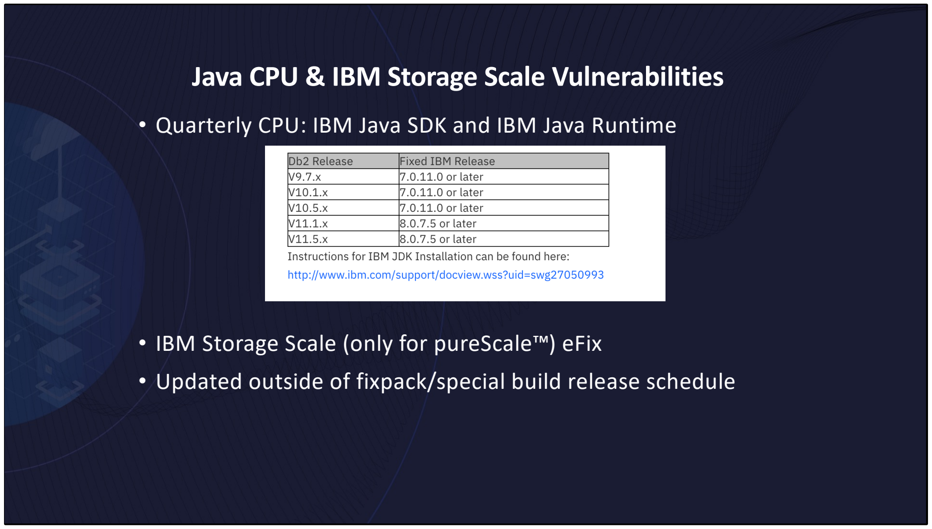
Remove the JMSAppender.class file via two options:
Here is the command:

```
   zip -d log4j-1.2.17.jar org/apache/log4j/net/JMSAppender.class
```

Each security bulletin has a “Workarounds and Mitigations” section. For most security bulletins, the only mitigation is to apply a fix.

However, in some instances steps to mitigate the vulnerability will be provided in this section. As an example, for the log4j vulnerability CVE-2021-4104, a mitigation for the vulnerability is to delete the JMSAppender class from the affected JAR file.

https://www.ibm.com/support/pages/node/6528678



Java CPU & IBM Storage Scale Vulnerabilities

- Quarterly CPU: IBM Java SDK and IBM Java Runtime

Db2 Release	Fixed IBM Release
V9.7.x	7.0.11.0 or later
V10.1.x	7.0.11.0 or later
V10.5.x	7.0.11.0 or later
V11.1.x	8.0.7.5 or later
V11.5.x	8.0.7.5 or later

Instructions for IBM JDK Installation can be found here:

http://www.ibm.com/support/docview.wss?uid=swg27050993

- IBM Storage Scale (only for pureScale™) eFix
- Updated outside of fixpack/special build release schedule

Java and Spectrum Scale/Storage Scale security fixes are released on a separate schedule than the fixpack/special build release schedule. Thus, a fix might be released in between fixpack or security SB releases. We do not generally include Java fixes in security special builds.

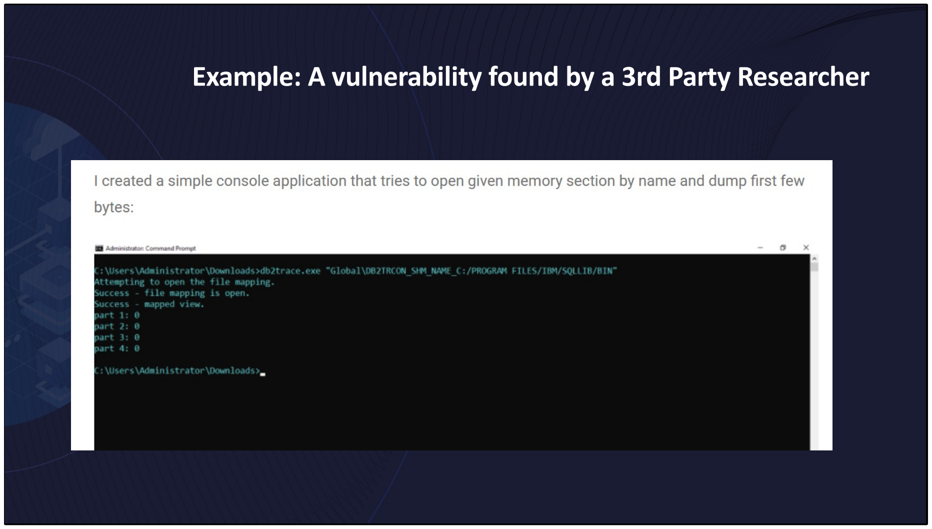
Java fixes are shipped on a quarterly basis. For Db2 10.5 on HP-UX, IBM JDK fixes are shipped twice a year instead.

Applying the Java fix is simple: download archive from FixCentral, unzip it into the correct directory to install, make changes to CLASSPATH and the JDK_PATH DBM CFG parameter.

Instructions for Java installation are in the following technote:
http://www.ibm.com/support/docview.wss?uid=swg27050993

IBM Storage Scale only affects AIX and Linux, and only for those customers who have Db2® pureScale™ feature installed.
IBM Storage Scale was previously called Spectrum Scale, and before that GPFS (General Parallel File System).
Instructions here: http://www-01.ibm.com/support/docview.wss?uid=swg27048484

4. A practical example of a published vulnerability



Example: A vulnerability found by a 3rd Party Researcher

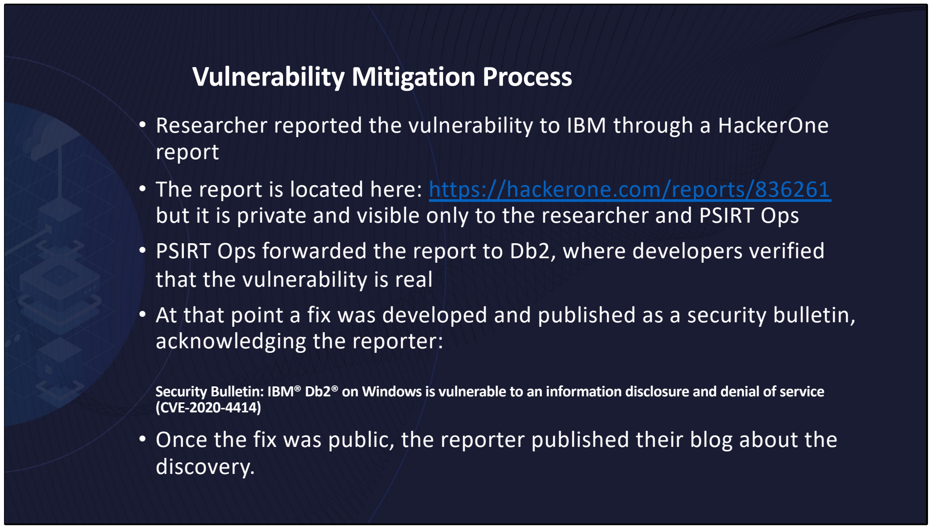
I created a simple console application that tries to open given memory section by name and dump first few bytes:

```
C:\Users\Administrator\Downloads>db2trace.exe "Global\DB2TRCON_SHM_NAME_C:/PROGRAM FILES/IBM/SQLLIB/BIN"
Attempting to open the file mapping.
Success - file mapping is open.
Success - mapped view.
part 1: 0
part 2: 0
part 3: 0
part 4: 0

C:\Users\Administrator\Downloads>
```

A practical example of the PSIRT process: a vulnerability researcher discovered an issue where trace memory regions on Windows were not properly protected. The image shows the researcher’s example where the first few bytes of the trace memory region are dumped by an unprivileged process.

Blog: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/ibm-db2-shared-memory-vulnerability-cve-2020-4414/



Vulnerability Mitigation Process

- Researcher reported the vulnerability to IBM through a HackerOne report
- The report is located here: https://hackerone.com/reports/836261 but it is private and visible only to the researcher and PSIRT Ops
- PSIRT Ops forwarded the report to Db2, where developers verified that the vulnerability is real
- At that point a fix was developed and published as a security bulletin, acknowledging the reporter:

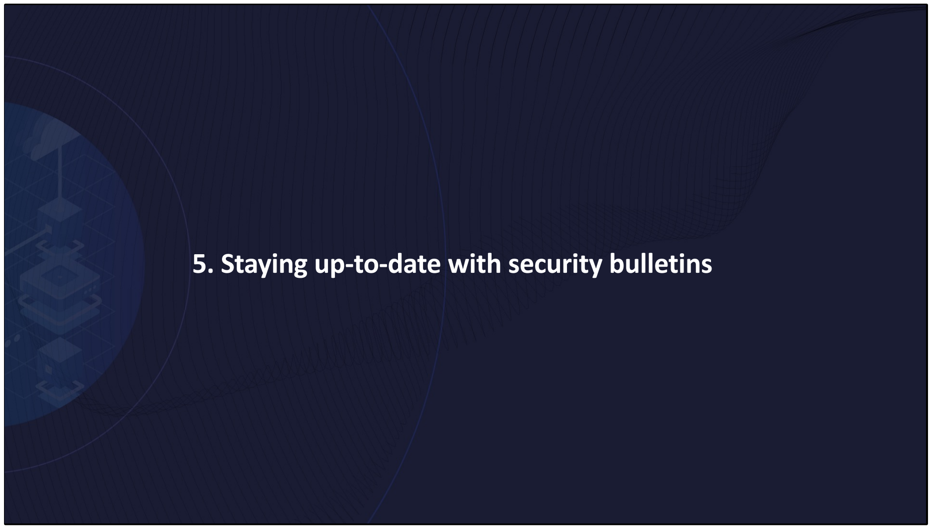
  Security Bulletin: IBM® Db2® on Windows is vulnerable to an information disclosure and denial of service (CVE-2020-4414)
- Once the fix was public, the reporter published their blog about the discovery.

In this instance, the vulnerability was reported through HackerOne. The report itself is private and only visible to the researcher and IBM PSIRT.

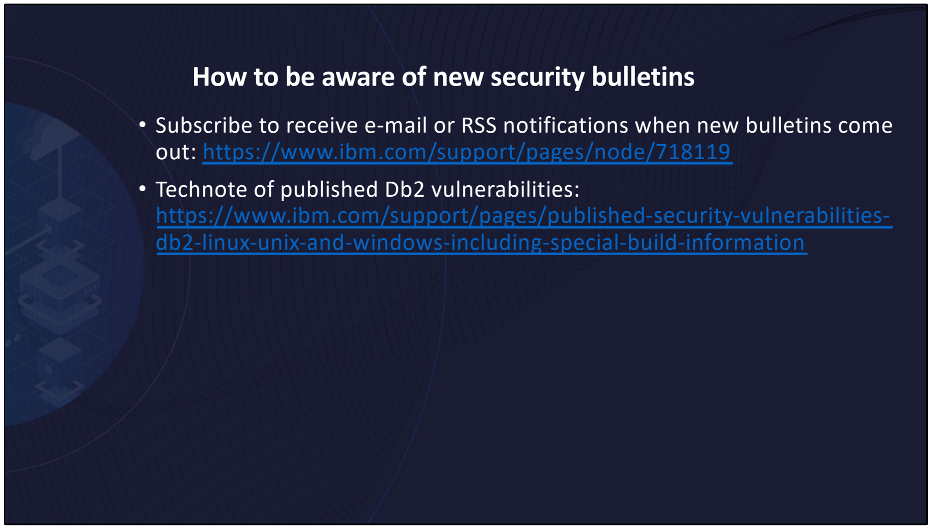
IBM PSIRT forwarded the report to DB2, where developers verified that the vulnerability is legitimate.

At that point a fix was developed, and a security bulletin was published, acknowledging the reporter.

Once the fix was public, the reporter published a blog post about the discovery.



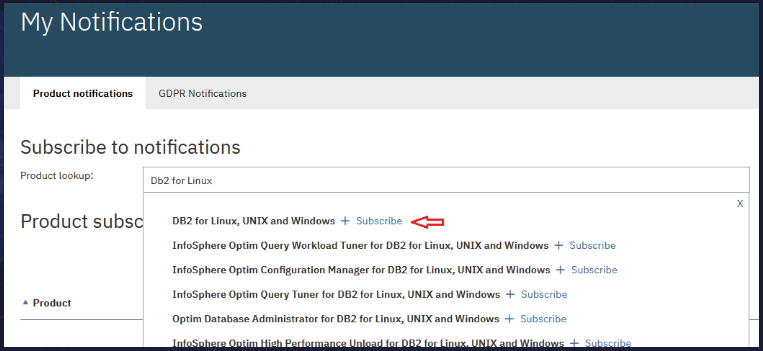
5. Staying up-to-date with security bulletins



How to be aware of new security bulletins

- Subscribe to receive e-mail or RSS notifications when new bulletins come out: https://www.ibm.com/support/pages/node/718119
- Technote of published Db2 vulnerabilities: https://www.ibm.com/support/pages/published-security-vulnerabilities-db2-linux-unix-and-windows-including-special-build-information

Subscribe to E-mail or RSS Feed Notifications



My Notifications

Product notifications | GDPR Notifications

Subscribe to notifications

Product lookup: Db2 for Linux

Product subsc

▲ Product

DB2 for Linux, UNIX and Windows + Subscribe

InfoSphere Optim Query Workload Tuner for DB2 for Linux, UNIX and Windows + Subscribe

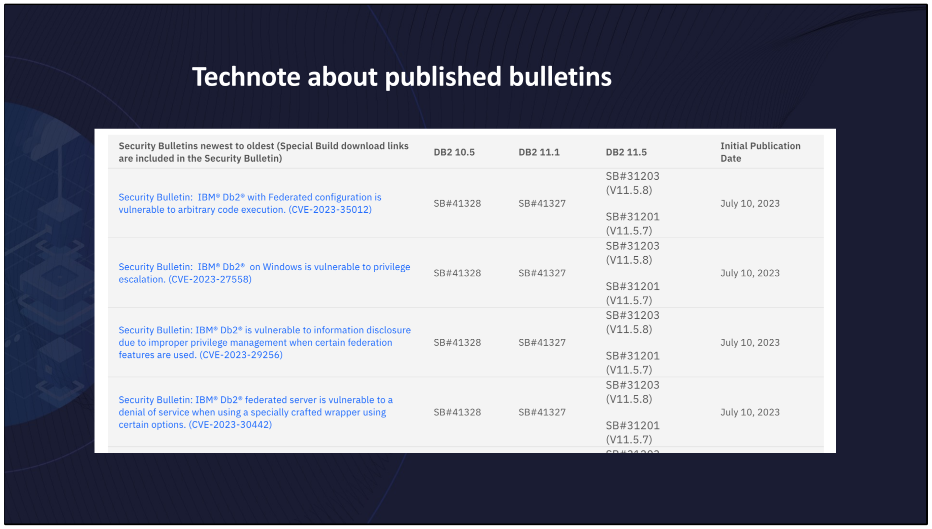
InfoSphere Optim Configuration Manager for DB2 for Linux, UNIX and Windows + Subscribe

InfoSphere Optim Query Tuner for DB2 for Linux, UNIX and Windows + Subscribe

Optim Database Administrator for DB2 for Linux, UNIX and Windows + Subscribe

InfoSphere Optim High Performance Unload for DB2 for Linux, UNIX and Windows + Subscribe

https://www.ibm.com/support/pages/my-notifications-subscription-service



Technote about published bulletins

Security Bulletins newest to oldest (Special Build download links are included in the Security Bulletin)	DB2 10.5	DB2 11.1	DB2 11.5	Initial Publication Date
Security Bulletin: IBM® Db2® with Federated configuration is vulnerable to arbitrary code execution. (CVE-2023-35012)	SB#41328	SB#41327	SB#31203 (V11.5.8) SB#31201 (V11.5.7)	July 10, 2023
Security Bulletin: IBM® Db2® on Windows is vulnerable to privilege escalation. (CVE-2023-27558)	SB#41328	SB#41327	SB#31203 (V11.5.8) SB#31201 (V11.5.7)	July 10, 2023
Security Bulletin: IBM® Db2® is vulnerable to information disclosure due to improper privilege management when certain federation features are used. (CVE-2023-29256)	SB#41328	SB#41327	SB#31203 (V11.5.8) SB#31201 (V11.5.7)	July 10, 2023
Security Bulletin: IBM® Db2® federated server is vulnerable to a denial of service when using a specially crafted wrapper using certain options. (CVE-2023-30442)	SB#41328	SB#41327	SB#31203 (V11.5.8) SB#31201 (V11.5.7)	July 10, 2023

Cumulative – latest sb always has all the previous
EoS (End of support) – fixes only available for later fixpacks
N/A – Not Affected
Solution on FixCentral – no special build available, customer can directly download the fix from FC.
SB = Special Build
New cumulative special build process for 11.5.* stream, includes all fixes not only security vulnerabilities.

Speaker: Mitchell Waite
Company: IBM
Email Address: mwaite@ibm.com

Thank you!