vul_files_45 Scan Report

Project Name	vul_files_45
Scan Start	Wednesday, January 8, 2025 10:05:28 AM
Preset	Checkmarx Default
Scan Time	01h:13m:01s
Lines Of Code Scanned	299394
Files Scanned	153
Report Creation Time	Wednesday, January 8, 2025 11:23:07 AM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	1/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

Included: Confirmed, Not Exploitable, To Verify, Urgent, Proposed Not Exploitable

Excluded: None

Assigned to

Included: All

Categories

Included:

Uncategorized	All
Custom	All
PCI DSS v3.2	All
OWASP Top 10 2013	All
FISMA 2014	All
NIST SP 800-53	All
OWASP Top 10 2017	All
OWASP Mobile Top 10 2016	All

Excluded:

Uncategorized	None
Custom	None
PCI DSS v3.2	None
OWASP Top 10 2013	None
FISMA 2014	None

NIST SP 800-53	None
OWASP Top 10 2017	None
OWASP Mobile Top 10 2016	None

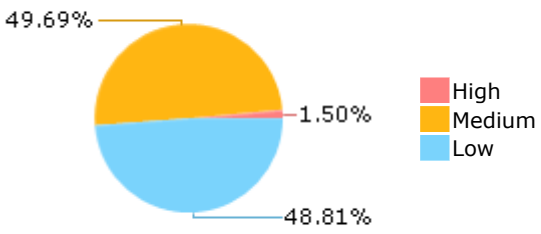
Results Limit

Results limit per query was set to 50

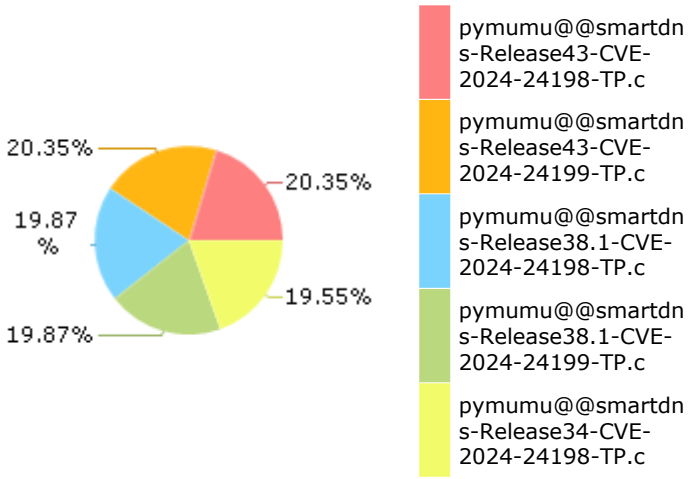
Selected Queries

Selected queries are listed in Result Summary

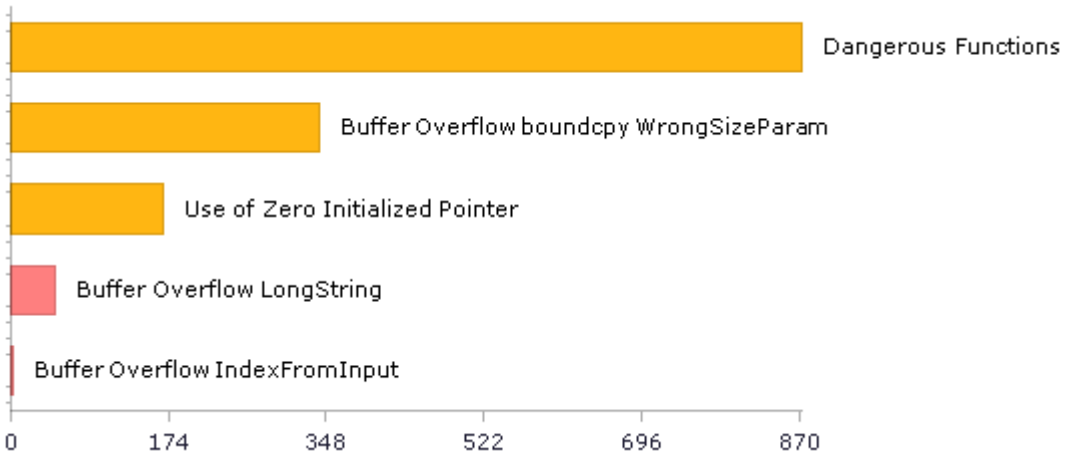
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2017

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	1025	529
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	318	318
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	26	18
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	873	873
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2013

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	18	10
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	873	873
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	2	2
PCI DSS (3.2) - 6.5.2 - Buffer overflows	418	388
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	41	41
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	113	113
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	281	281
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	26	18
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	17	17

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	431	431
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	12	12
SC-4 Information in Shared Resources (P1)	4	4
SC-5 Denial of Service Protection (P1)*	1041	502
SC-8 Transmission Confidentiality and Integrity (P1)	14	6
SI-10 Information Input Validation (P1)*	95	65
SI-11 Error Handling (P2)*	398	398
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	29	29

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly.	0	0
M6-Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	0	0
M8-Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.	0	0
M10-Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.	0	0

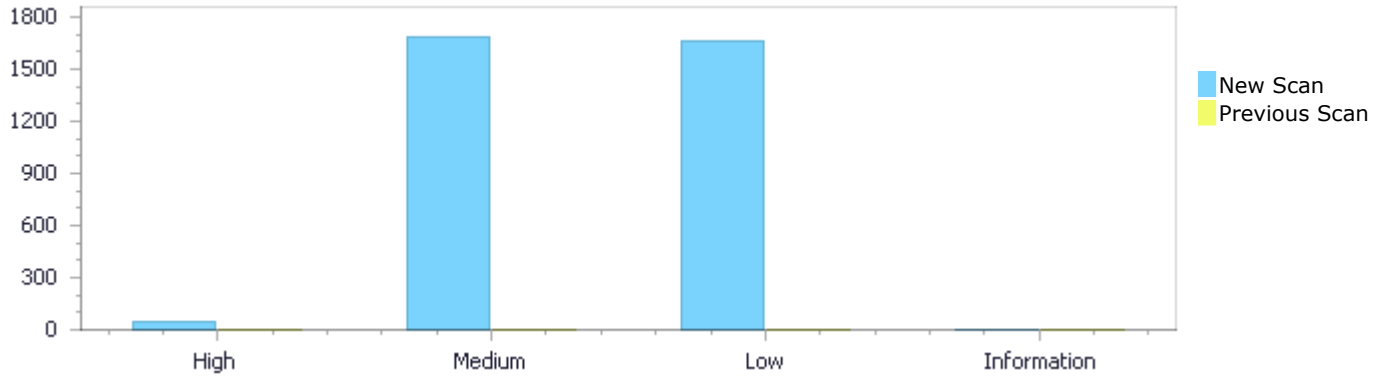
Scan Summary - Custom

Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	51	1,689	1,659	0	3,399
Recurrent Issues	0	0	0	0	0
Total	51	1,689	1,659	0	3,399
Fixed Issues	0	0	0	0	0



Results Distribution By State

	High	Medium	Low	Information	Total
Confirmed	0	0	0	0	0
Not Exploitable	0	0	0	0	0
To Verify	51	1,689	1,659	0	3,399
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	51	1,689	1,659	0	3,399

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow LongString	49	High
Buffer Overflow IndexFromInput	2	High
Dangerous Functions	873	Medium
Buffer Overflow boundcpy WrongSizeParam	341	Medium
Use of Zero Initialized Pointer	168	Medium

Memory Leak	154	Medium
Wrong Size t Allocation	42	Medium
MemoryFree on StackVariable	36	Medium
Double Free	19	Medium
Use of Uninitialized Pointer	17	Medium
Short Overflow	11	Medium
Off by One Error in Methods	8	Medium
Integer Overflow	6	Medium
Use of Uninitialized Variable	6	Medium
Heap Inspection	4	Medium
Char Overflow	3	Medium
Stored Buffer Overflow fgets	1	Medium
NULL Pointer Dereference	622	Low
Unchecked Return Value	398	Low
Improper Resource Access Authorization	277	Low
Exposure of System Data to Unauthorized Control Sphere	113	Low
Unreleased Resource Leak	74	Low
TOCTOU	50	Low
Incorrect Permission Assignment For Critical Resources	41	Low
Unchecked Array Index	25	Low
Use of Sizeof On a Pointer Type	17	Low
Insufficiently Protected Credentials	14	Low
Sizeof Pointer Argument	10	Low
Use of Insufficiently Random Values	8	Low
Inconsistent Implementations	4	Low
Information Exposure Through Comments	4	Low
Potential Off by One Error in Loops	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	85
postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	84
pymumu@@smartdns-Release45-CVE-2023-31470-FP.c	55
pymumu@@smartdns-Release46-CVE-2023-31470-FP.c	55
postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	52
postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	52
pymumu@@smartdns-Release43-CVE-2023-31470-FP.c	41
protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c	40
protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c	40
pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	38

Scan Results Details

Buffer Overflow LongString

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow LongString Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 811 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Line	814	592
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
814.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
592.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=2
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 811 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Line	814	594
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
814.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 811 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Line	856	594
Object	"\xff\xa3"	tmp

Code Snippet
File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=4
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 811 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Line	856	592
Object	"\xff\xa3"	tmp

Code Snippet

File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
592.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=5
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 811 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Line	814	592
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name php@@php-src-php-8.0.25-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
814.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.0.25-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
592.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=6
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 811 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Line	814	594
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
814.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Method	static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=7
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 811 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Line	856	594
Object	"\xff\xa3"	tmp

Code Snippet

File Name	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Method	static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=8
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 811 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Line	856	592
Object	"\xff\xa3"	tmp

Code Snippet

File Name php@@php-src-php-8.0.25-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.0.25-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
592.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=9
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 811 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Line	814	594
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
814.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=10
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 811 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Line	814	592
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
814.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
592.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=11
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 811 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Line	856	592
Object	"\xff\xa3"	tmp

Code Snippet

File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
592.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=12
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 811 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Line	856	594
Object	"\xff\xa3"	tmp

Code Snippet
File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=13
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 803 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Line	806	584
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
806.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
584.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=14
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 803 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Line	806	586
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
806.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
586.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=15
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 803 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Line	848	584

Object	"\xff\xa3"	tmp

Code Snippet
File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
848.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
584.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=16
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 803 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Line	848	586
Object	"\xff\xa3"	tmp

Code Snippet
File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
848.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
586.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=17
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 811 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Line	814	592
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name php@@php-src-php-8.1.8-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
814.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.1.8-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
592.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=18
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 811 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Line	814	594
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
814.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=19
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 811 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Line	856	592
Object	"\xff\xa3"	tmp

Code Snippet
File Name php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method	static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
592.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=20
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 811 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Line	856	594
Object	"\xff\xa3"	tmp

Code Snippet

File Name	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method	static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=21
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 803 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Line	806	584
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
806.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
584.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=22
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 803 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Line	806	586
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
806.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
586.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=23
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 803 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Line	848	584
Object	"\xff\xa3"	tmp

Code Snippet

File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
848.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
584.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=24
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 803 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Line	848	586
Object	"\xff\xa3"	tmp

Code Snippet

File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
848.                const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
586.                        tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=25
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 803 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Line	806	584
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
806.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method	static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
584.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=26
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 803 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Line	806	586
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
806.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method	static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
586.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 27:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=27
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 803 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Line	848	584
Object	"\xff\xa3"	tmp

Code Snippet

File Name php@@php-src-php-8.2.18-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
848.                const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.2.18-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
584.                        tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=28
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 803 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Line	848	586
Object	"\xff\xa3"	tmp

Code Snippet

File Name php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
848.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
586.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=29
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 803 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Line	806	584
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
806.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
584.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 30:

Severity High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=30
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 803 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Line	806	586
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
806.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
586.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=31
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 803 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Line	848	584
Object	"\xff\xa3"	tmp

Code Snippet
File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
848.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
584.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=32
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 803 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Line	848	586
Object	"\xff\xa3"	tmp

Code Snippet
File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
848.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
586.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=33
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 811 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Line	814	594
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet

File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
814.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=34
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 811 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Line	814	592

Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
814.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
592.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=35
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 811 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Line	856	592
Object	"\xff\xa3"	tmp

Code Snippet
File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.            const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
592.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=36
Status	New

The size of the buffer used by BF_set_key in tmp, at line 541 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 811 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Line	856	594
Object	"\xff\xa3"	tmp

Code Snippet

File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
594.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=37
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 803 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c

Line	806	586
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
806.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
586.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=38
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "8b \xd0\xc1\xd2\xcf\xcc\xd8", at line 803 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Line	806	584
Object	"8b \xd0\xc1\xd2\xcf\xcc\xd8"	tmp

Code Snippet
File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
806.        const char *test_key = "8b \xd0\xc1\xd2\xcf\xcc\xd8";
```

File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
584.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=39
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 803 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Line	848	586
Object	"\xff\xa3"	tmp

Code Snippet

File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c

Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
848.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
586.                    tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=40
Status	New

The size of the buffer used by BF_set_key in tmp, at line 533 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to "\xff\xa3", at line 803 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Line	848	584
Object	"\xff\xa3"	tmp

Code Snippet
File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
848.              const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```

File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
584.                    tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=41
Status	New

The size of the buffer used by get_available_versions_for_extension in values, at line 1913 of postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_extension_control_directory passes to "%s/extension", at line 353 of postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	360	1962
Object	"%s/extension"	values

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method get_extension_control_directory(void)

```
....
360.        snprintf(result, MAXPGPATH, "%s/extension", sharepath);
```

File Name	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method	get_available_versions_for_extension(ExtensionControlFile *pcontrol,

```
....
1962.             values[1] = CStringGetTextDatum(vername);
```

Buffer Overflow LongString\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=42
Status	New

The size of the buffer used by backend_forkexec in av, at line 4383 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that backend_forkexec passes to "postgres", at line 4383 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4388	4388
Object	"postgres"	av

Code Snippet

File Name	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method	backend_forkexec(Port *port)

```
....
4388.       av[ac++] = "postgres";
```

Buffer Overflow LongString\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=43
Status	New

The size of the buffer used by backend_forkexec in av, at line 4383 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that backend_forkexec passes to "--forkbackend", at line 4383 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4389	4389
Object	"--forkbackend"	av

Code Snippet	
File Name	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method	backend_forkexec(Port *port)

```
....
4389.       av[ac++] = "--forkbackend";
```

Buffer Overflow LongString\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=44
Status	New

The size of the buffer used by StartChildProcess in av, at line 5272 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that StartChildProcess passes to "--forkboot", at line 5272 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5285	5285
Object	"--forkboot"	av

Code Snippet	
File Name	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method	StartChildProcess(AuxProcType type)

```
....
5285.       av[ac++] = "--forkboot";
```

Buffer Overflow LongString\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=45
Status	New

The size of the buffer used by bgworker_forkexec in av, at line 5588 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgworker_forkexec passes to "--forkbgworker=%d", at line 5588 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5594	5597

Object	"--forkbgworker=%d"	av

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method bgworker_forkexec(int shmem_slot)

```
....
5594.       snprintf(forkav, MAXPGPATH, "--forkbgworker=%d",
shmem_slot);
....
5597.       av[ac++] = forkav;
```

Buffer Overflow LongString\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=46
Status	New

The size of the buffer used by backend_forkexec in av, at line 4419 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that backend_forkexec passes to "postgres", at line 4419 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	4424	4424
Object	"postgres"	av

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method backend_forkexec(Port *port)

```
....
4424.       av[ac++] = "postgres";
```

Buffer Overflow LongString\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=47
Status	New

The size of the buffer used by backend_forkexec in av, at line 4419 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that backend_forkexec passes to "--forkbackend", at line 4419 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination

File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	4425	4425
Object	"--forkbackend"	av

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method backend_forkexec(Port *port)

```
....
4425.        av[ac++] = "--forkbackend";
```

Buffer Overflow LongString\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=48
Status	New

The size of the buffer used by StartChildProcess in av, at line 5351 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that StartChildProcess passes to "--forkboot", at line 5351 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5364	5364
Object	"--forkboot"	av

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method StartChildProcess(AuxProcType type)

```
....
5364.        av[ac++] = "--forkboot";
```

Buffer Overflow LongString\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=49
Status	New

The size of the buffer used by bgworker_forkexec in av, at line 5667 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgworker_forkexec passes to "--forkbgworker=%d", at line 5667 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5673	5676
Object	"--forkbgworker=%d"	av

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method bgworker_forkexec(int shmem_slot)

```
....
5673.       snprintf(forkav, MAXPGPATH, "--forkbgworker=%d",
shmem_slot);
....
5676.       av[ac++] = forkav;
```

Buffer Overflow IndexFromInput

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow IndexFromInput Version:1

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=50
Status	New

The size of the buffer used by parseServiceFile in i, at line 4067 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseServiceFile passes to fgets, at line 4067 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	4087	4198
Object	fgets	i

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method parseServiceFile(const char *serviceFile,

```
....
4087.       while ((line = fgets(buf, sizeof(buf), f)) != NULL)
....
4198.                                                   options[i].val =
strdup(val);
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=51
Status	New

The size of the buffer used by parseServiceFile in i, at line 4070 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseServiceFile passes to fgets, at line 4070 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	4090	4201
Object	fgets	i

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method parseServiceFile(const char *serviceFile,

```
....
4090.       while ((line = fgets(buf, sizeof(buf), f)) != NULL)
....
4201.                                                   options[i].val =
strdup(val);
```

Dangerous Functions

Query Path:
CPP\Cx\CPP Medium Threat\Dangerous Functions Version:1

Categories

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities

Description

Dangerous Functions\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1151
Status	New

The dangerous function, memcpy, was found in use at line 811 in php@@php-src-php-8.0.17-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Line	840	840
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
840.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1152
Status New

The dangerous function, memcpy, was found in use at line 647 in php@@php-src-php-8.0.17-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Line	693	693
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
693.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1153
Status New

The dangerous function, memcpy, was found in use at line 647 in php@@php-src-php-8.0.17-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Line	763	763
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
763.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1154
Status	New

The dangerous function, memcpy, was found in use at line 811 in php@@php-src-php-8.0.25-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Line	840	840
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
840.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1155

Status	New

The dangerous function, memcpy, was found in use at line 647 in php@@php-src-php-8.0.25-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Line	693	693
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
693.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1156
Status	New

The dangerous function, memcpy, was found in use at line 647 in php@@php-src-php-8.0.25-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Line	763	763
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
763.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=1157
Status	New

The dangerous function, memcpy, was found in use at line 811 in php@@php-src-php-8.0.5-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Line	840	840
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
840.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1158
Status	New

The dangerous function, memcpy, was found in use at line 647 in php@@php-src-php-8.0.5-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Line	693	693
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
693.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1159
Status	New

The dangerous function, memcpy, was found in use at line 647 in php@@php-src-php-8.0.5-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Line	763	763
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
763.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1160
Status	New

The dangerous function, memcpy, was found in use at line 803 in php@@php-src-php-8.1.27-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Line	832	832
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
832.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1161
Status	New

The dangerous function, memcpy, was found in use at line 639 in php@@php-src-php-8.1.27-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Line	685	685
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
685.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1162
Status	New

The dangerous function, memcpy, was found in use at line 639 in php@@php-src-php-8.1.27-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Line	755	755
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
755.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 13:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1163
Status	New

The dangerous function, memcpy, was found in use at line 811 in php@@php-src-php-8.1.8-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Line	840	840
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
840.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1164
Status	New

The dangerous function, memcpy, was found in use at line 647 in php@@php-src-php-8.1.8-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Line	693	693
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
693.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1165
Status	New

The dangerous function, memcpy, was found in use at line 647 in php@@php-src-php-8.1.8-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Line	763	763
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
763.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1166
Status	New

The dangerous function, memcpy, was found in use at line 803 in php@@php-src-php-8.2.10-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Line	832	832
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
832.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1167
Status	New

The dangerous function, memcpy, was found in use at line 639 in php@@php-src-php-8.2.10-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Line	685	685
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
685.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1168
Status	New

The dangerous function, memcpy, was found in use at line 639 in php@@php-src-php-8.2.10-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Line	755	755
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
755.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1169
Status	New

The dangerous function, memcpy, was found in use at line 803 in php@@php-src-php-8.2.18-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Line	832	832
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
832.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1170
Status	New

The dangerous function, memcpy, was found in use at line 639 in php@@php-src-php-8.2.18-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Line	685	685
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
685.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1171
Status	New

The dangerous function, memcpy, was found in use at line 639 in php@@php-src-php-8.2.18-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Line	755	755
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
755.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1172
Status	New

The dangerous function, memcpy, was found in use at line 803 in php@@php-src-php-8.2.22-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Line	832	832
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c

Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
832.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1173
Status	New

The dangerous function, memcpy, was found in use at line 639 in php@@php-src-php-8.2.22-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Line	685	685
Object	memcpy	memcpy

Code Snippet	
File Name	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Method	static char *BF_crypt(const char *key, const char *setting,

```
....
685.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1174
Status	New

The dangerous function, memcpy, was found in use at line 639 in php@@php-src-php-8.2.22-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Line	755	755
Object	memcpy	memcpy

Code Snippet

File Name	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Method	static char *BF_crypt(const char *key, const char *setting,

```
....
755.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1175
Status	New

The dangerous function, memcpy, was found in use at line 811 in php@@php-src-php-8.2.2-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Line	840	840
Object	memcpy	memcpy

Code Snippet

File Name	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
840.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1176
Status	New

The dangerous function, memcpy, was found in use at line 647 in php@@php-src-php-8.2.2-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Line	693	693
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
693.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1177
Status	New

The dangerous function, memcpy, was found in use at line 647 in php@@php-src-php-8.2.2-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Line	763	763
Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
763.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1178
Status	New

The dangerous function, memcpy, was found in use at line 803 in php@@php-src-php-8.2.6-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Line	832	832
Object	memcpy	memcpy

Code Snippet	
File Name	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
832.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1179
Status	New

The dangerous function, memcpy, was found in use at line 639 in php@@php-src-php-8.2.6-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Line	685	685
Object	memcpy	memcpy

Code Snippet	
File Name	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method	static char *BF_crypt(const char *key, const char *setting,

```
....
685.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1180
Status	New

The dangerous function, memcpy, was found in use at line 639 in php@@php-src-php-8.2.6-CVE-2020-1916-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Line	755	755

Object	memcpy	memcpy

Code Snippet
File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
755.        memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1181
Status	New

The dangerous function, memcpy, was found in use at line 980 in pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Line	1059	1059
Object	memcpy	memcpy

Code Snippet
File Name pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Method int task_decoder_update(davs2_t *h)

```
....
1059.      memcpy(h->wq.seq_wq_matrix, seq->seq_wq_matrix, 2 * 64 *
sizeof(int16_t)); /* weighting quantization matrix */
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1182
Status	New

The dangerous function, memcpy, was found in use at line 980 in pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c

Line	1060	1060
Object	memcpy	memcpy

Code Snippet
File Name pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Method int task_decoder_update(davs2_t *h)

```
....
1060.       memcpy(&h->seq_info, seq, sizeof(davs2_seq_t));
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1183
Status	New

The dangerous function, memcpy, was found in use at line 1068 in pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Line	1079	1079
Object	memcpy	memcpy

Code Snippet
File Name pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Method int task_set_sequence_head(davs2_mgr_t *mgr, davs2_seq_t *seq)

```
....
1079.           memcpy(&mgr->seq_info, seq, sizeof(davs2_seq_t));
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1184
Status	New

The dangerous function, memcpy, was found in use at line 618 in postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-	postgres@@postgres-REL9_6_18-CVE-

	2020-14350-TP.c	2020-14350-TP.c
Line	627	627
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method read_extension_aux_control_file(const ExtensionControlFile *pcontrol,

```
....
627.        memcpy(acontrol, pcontrol, sizeof(ExtensionControlFile));
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1185
Status	New

The dangerous function, memcpy, was found in use at line 1493 in postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	1561	1561
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method RelationBuildTriggers(Relation relation)

```
....
1561.                   memcpy(build->tgattr, &(pg_trigger-
>tgattr.values),
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1186
Status	New

The dangerous function, memcpy, was found in use at line 1691 in postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	1701	1701
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method CopyTriggerDesc(TriggerDesc *trigdesc)

```
....
1701.       memcpy(newdesc, trigdesc, sizeof(TriggerDesc));
```

Dangerous Functions\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1187
Status New

The dangerous function, memcpy, was found in use at line 1691 in postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	1704	1704
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method CopyTriggerDesc(TriggerDesc *trigdesc)

```
....
1704.       memcpy(trigger, trigdesc->triggers,
```

Dangerous Functions\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1188
Status New

The dangerous function, memcpy, was found in use at line 1691 in postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	1716	1716
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method CopyTriggerDesc(TriggerDesc *trigdesc)

```
....
1716.                   memcpy(newattr, trigger->tgattr,
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1189
Status	New

The dangerous function, memcpy, was found in use at line 3320 in postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	3419	3419
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method afterTriggerAddEvent(AfterTriggerEventList *events,

```
....
3419.       memcpy(newevent, event, eventsize);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1190
Status	New

The dangerous function, memcpy, was found in use at line 4444 in postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	4453	4453
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method SetConstraintStateCopy(SetConstraintState origstate)

```
....
4453.       memcpy(state->trigstates, origstate->trigstates,
```

Dangerous Functions\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1191
Status New

The dangerous function, memcpy, was found in use at line 1638 in postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	1665	1665
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method ServerLoop(void)

```
....
1665.              memcpy((char *) &rmask, (char *) &readmask,
sizeof(fd_set));
```

Dangerous Functions\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1192
Status New

The dangerous function, memcpy, was found in use at line 5617 in postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5676	5676
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method do_start_bgworker(RegisteredBgWorker *rw)

```
....
5676.                   memcpy(MyBgworkerEntry, &rw->rw_worker,
sizeof(BackgroundWorker));
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1193
Status	New

The dangerous function, memcpy, was found in use at line 5974 in postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5981	5981
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method save_backend_variables(BackendParameters *param, Port *port)

```
....
5981.       memcpy(&param->port, port, sizeof(Port));
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1194

Status	New

The dangerous function, memcpy, was found in use at line 5974 in postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5987	5987
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method save_backend_variables(BackendParameters *param, Port *port)

```
....
5987.       memcpy(&param->ListenSocket, &ListenSocket,
sizeof(ListenSocket));
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1195
Status	New

The dangerous function, memcpy, was found in use at line 5974 in postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	6038	6038
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method save_backend_variables(BackendParameters *param, Port *port)

```
....
6038.       memcpy(&param->syslogPipe, &syslogPipe, sizeof(syslogPipe));
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1196
Status	New

The dangerous function, memcpy, was found in use at line 6216 in postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	6218	6218
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method restore_backend_variables(BackendParameters *param, Port *port)

```
....
6218.       memcpy(port, &param->port, sizeof(Port));
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1197
Status	New

The dangerous function, memcpy, was found in use at line 6216 in postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	6223	6223
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method restore_backend_variables(BackendParameters *param, Port *port)

```
....
6223.       memcpy(&ListenSocket, &param->ListenSocket,
sizeof(ListenSocket));
```

Dangerous Functions\Path 48:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1198
Status	New

The dangerous function, memcpy, was found in use at line 6216 in postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	6270	6270
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method restore_backend_variables(BackendParameters *param, Port *port)

```
....
6270.       memcpy(&syslogPipe, &param->syslogPipe, sizeof(syslogPipe));
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1199
Status	New

The dangerous function, memcpy, was found in use at line 1738 in postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	1890	1890
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
1890.                                   memcpy(&conn->raddr.addr, addr_cur-
>ai_addr,
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1200
Status	New

The dangerous function, memcpy, was found in use at line 3266 in postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	3280	3280
Object	memcpy	memcpy

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQgetCancel(PGconn *conn)

```
....
3280.       memcpy(&cancel->raddr, &conn->raddr, sizeof(SockAddr));
```

Buffer Overflow boundcpy WrongSizeParam

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundcpy WrongSizeParam Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow boundcpy WrongSizeParam\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=52
Status	New

The size of the buffer used by *php_crypt_blowfish_rn in Namespace1123564465, at line 811 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to Namespace1123564465, at line 811 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Line	840	840

Object	Namespace1123564465	Namespace1123564465

Code Snippet
File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
840.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=53
Status	New

The size of the buffer used by *BF_crypt in Namespace1123564465, at line 647 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace1123564465, at line 647 of php@@php-src-php-8.0.17-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Line	693	693
Object	Namespace1123564465	Namespace1123564465

Code Snippet
File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
693.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=54
Status	New

The size of the buffer used by *php_crypt_blowfish_rn in Namespace185884152, at line 811 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to Namespace185884152, at line 811 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.25-CVE-2020-	php@@php-src-php-8.0.25-CVE-2020-

	1916-TP.c	1916-TP.c
Line	840	840
Object	Namespace185884152	Namespace185884152

Code Snippet
File Name php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
840.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=55
Status	New

The size of the buffer used by *BF_crypt in Namespace185884152, at line 647 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace185884152, at line 647 of php@@php-src-php-8.0.25-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Line	693	693
Object	Namespace185884152	Namespace185884152

Code Snippet
File Name php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
693.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=56
Status	New

The size of the buffer used by *php_crypt_blowfish_rn in Namespace931889764, at line 811 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to Namespace931889764, at line 811 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Line	840	840
Object	Namespace931889764	Namespace931889764

Code Snippet
File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
840.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=57
Status New

The size of the buffer used by *BF_crypt in Namespace931889764, at line 647 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace931889764, at line 647 of php@@php-src-php-8.0.5-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Line	693	693
Object	Namespace931889764	Namespace931889764

Code Snippet
File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
693.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=58
Status New

The size of the buffer used by *php_crypt_blowfish_rn in Namespace2001996657, at line 803 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to

Namespace2001996657, at line 803 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Line	832	832
Object	Namespace2001996657	Namespace2001996657

Code Snippet
File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
832.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=59
Status New

The size of the buffer used by *BF_crypt in Namespace2001996657, at line 639 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace2001996657, at line 639 of php@@php-src-php-8.1.27-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Line	685	685
Object	Namespace2001996657	Namespace2001996657

Code Snippet
File Name php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
685.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=60
Status New

The size of the buffer used by *php_crypt_blowfish_rn in Namespace913496840, at line 811 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to Namespace913496840, at line 811 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Line	840	840
Object	Namespace913496840	Namespace913496840

Code Snippet
File Name php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
840.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=61
Status New

The size of the buffer used by *BF_crypt in Namespace913496840, at line 647 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace913496840, at line 647 of php@@php-src-php-8.1.8-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Line	693	693
Object	Namespace913496840	Namespace913496840

Code Snippet
File Name php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
693.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=62

Status	New

The size of the buffer used by *php_crypt_blowfish_rn in Namespace839693866, at line 803 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to Namespace839693866, at line 803 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Line	832	832
Object	Namespace839693866	Namespace839693866

Code Snippet
File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
832.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=63
Status	New

The size of the buffer used by *BF_crypt in Namespace839693866, at line 639 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace839693866, at line 639 of php@@php-src-php-8.2.10-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Line	685	685
Object	Namespace839693866	Namespace839693866

Code Snippet
File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
685.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=64
Status	New

The size of the buffer used by *php_crypt_blowfish_rn in Namespace1995103746, at line 803 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to Namespace1995103746, at line 803 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Line	832	832
Object	Namespace1995103746	Namespace1995103746

Code Snippet
File Name php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
832.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=65
Status	New

The size of the buffer used by *BF_crypt in Namespace1995103746, at line 639 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace1995103746, at line 639 of php@@php-src-php-8.2.18-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Line	685	685
Object	Namespace1995103746	Namespace1995103746

Code Snippet
File Name php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
685.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=66
Status	New

The size of the buffer used by *php_crypt_blowfish_rn in Namespace1847536225, at line 803 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to Namespace1847536225, at line 803 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Line	832	832
Object	Namespace1847536225	Namespace1847536225

Code Snippet
File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
832.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=67
Status	New

The size of the buffer used by *BF_crypt in Namespace1847536225, at line 639 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace1847536225, at line 639 of php@@php-src-php-8.2.22-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Line	685	685
Object	Namespace1847536225	Namespace1847536225

Code Snippet
File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
685.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=68
Status	New

The size of the buffer used by *php_crypt_blowfish_rn in Namespace337193279, at line 811 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to Namespace337193279, at line 811 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Line	840	840
Object	Namespace337193279	Namespace337193279

Code Snippet
File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
840.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=69
Status	New

The size of the buffer used by *BF_crypt in Namespace337193279, at line 647 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace337193279, at line 647 of php@@php-src-php-8.2.2-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Line	693	693
Object	Namespace337193279	Namespace337193279

Code Snippet
File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Method static char *BF_crypt(const char *key, const char *setting,

```
....
693.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=70
Status	New

The size of the buffer used by *php_crypt_blowfish_rn in Namespace1701636291, at line 803 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *php_crypt_blowfish_rn passes to Namespace1701636291, at line 803 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Line	832	832
Object	Namespace1701636291	Namespace1701636291

Code Snippet
File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
832.        memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=71
Status	New

The size of the buffer used by *BF_crypt in Namespace1701636291, at line 639 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace1701636291, at line 639 of php@@php-src-php-8.2.6-CVE-2020-1916-TP.c, to overwrite the target buffer.

	Source	Destination
File	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Line	685	685
Object	Namespace1701636291	Namespace1701636291

Code Snippet

File Name	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method	static char *BF_crypt(const char *key, const char *setting,

```
....
685.        memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=72
Status	New

The size of the buffer used by task_decoder_update in davs2_seq_t, at line 980 of pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that task_decoder_update passes to davs2_seq_t, at line 980 of pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c, to overwrite the target buffer.

	Source	Destination
File	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Line	1060	1060
Object	davs2_seq_t	davs2_seq_t

Code Snippet

File Name	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Method	int task_decoder_update(davs2_t *h)

```
....
1060.       memcpy(&h->seq_info, seq, sizeof(davs2_seq_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=73
Status	New

The size of the buffer used by task_set_sequence_head in davs2_seq_t, at line 1068 of pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that task_set_sequence_head passes to davs2_seq_t, at line 1068 of pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c, to overwrite the target buffer.

	Source	Destination
File	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Line	1079	1079
Object	davs2_seq_t	davs2_seq_t

Code Snippet	
File Name	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Method	int task_set_sequence_head(davs2_mgr_t *mgr, davs2_seq_t *seq)

```
....
1079.          memcpy(&mgr->seq_info, seq, sizeof(davs2_seq_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=74
Status	New

The size of the buffer used by read_extension_aux_control_file in ExtensionControlFile, at line 618 of postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_extension_aux_control_file passes to ExtensionControlFile, at line 618 of postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	627	627
Object	ExtensionControlFile	ExtensionControlFile

Code Snippet	
File Name	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method	read_extension_aux_control_file(const ExtensionControlFile *pcontrol,

```
....
627.        memcpy(acontrol, pcontrol, sizeof(ExtensionControlFile));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=75
Status	New

The size of the buffer used by CopyTriggerDesc in TriggerDesc, at line 1691 of postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CopyTriggerDesc passes to TriggerDesc, at line 1691 of postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	1701	1701

Object	TriggerDesc	TriggerDesc

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method CopyTriggerDesc(TriggerDesc *trigdesc)

```
....
1701.       memcpy(newdesc, trigdesc, sizeof(TriggerDesc));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=76
Status	New

The size of the buffer used by ServerLoop in fd_set, at line 1638 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ServerLoop passes to fd_set, at line 1638 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	1665	1665
Object	fd_set	fd_set

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method ServerLoop(void)

```
....
1665.             memcpy((char *) &rmask, (char *) &readmask,
sizeof(fd_set));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=77
Status	New

The size of the buffer used by do_start_bgworker in BackgroundWorker, at line 5617 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that do_start_bgworker passes to BackgroundWorker, at line 5617 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-	postgres@@postgres-REL9_6_18-CVE-

	2021-23214-TP.c	2021-23214-TP.c
Line	5676	5676
Object	BackgroundWorker	BackgroundWorker

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method do_start_bgworker(RegisteredBgWorker *rw)

```
....
5676.                   memcpy(MyBgworkerEntry, &rw->rw_worker,
sizeof(BackgroundWorker));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=78
Status	New

The size of the buffer used by save_backend_variables in Port, at line 5974 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that save_backend_variables passes to Port, at line 5974 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5981	5981
Object	Port	Port

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method save_backend_variables(BackendParameters *param, Port *port)

```
....
5981.       memcpy(&param->port, port, sizeof(Port));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=79
Status	New

The size of the buffer used by save_backend_variables in ListenSocket, at line 5974 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that save_backend_variables passes to ListenSocket, at line 5974 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5987	5987
Object	ListenSocket	ListenSocket

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method save_backend_variables(BackendParameters *param, Port *port)

```
....
5987.       memcpy(&param->ListenSocket, &ListenSocket,
sizeof(ListenSocket));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=80
Status	New

The size of the buffer used by save_backend_variables in syslogPipe, at line 5974 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that save_backend_variables passes to syslogPipe, at line 5974 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	6038	6038
Object	syslogPipe	syslogPipe

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method save_backend_variables(BackendParameters *param, Port *port)

```
....
6038.       memcpy(&param->syslogPipe, &syslogPipe, sizeof(syslogPipe));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=81
Status	New

The size of the buffer used by restore_backend_variables in Port, at line 6216 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable

a buffer overflow attack, using the source buffer that restore_backend_variables passes to Port, at line 6216 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	6218	6218
Object	Port	Port

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method restore_backend_variables(BackendParameters *param, Port *port)

```
....
6218.       memcpy(port, &param->port, sizeof(Port));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=82
Status	New

The size of the buffer used by PQgetCancel in SockAddr, at line 3266 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that PQgetCancel passes to SockAddr, at line 3266 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	3280	3280
Object	SockAddr	SockAddr

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQgetCancel(PGconn *conn)

```
....
3280.       memcpy(&cancel->raddr, &conn->raddr, sizeof(SockAddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=83
Status	New

The size of the buffer used by ServerLoop in fd_set, at line 1657 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ServerLoop passes to fd_set, at line 1657 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	1684	1684
Object	fd_set	fd_set

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method ServerLoop(void)

```
....
1684.             memcpy((char *) &rmask, (char *) &readmask,
sizeof(fd_set));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=84
Status New

The size of the buffer used by do_start_bgworker in BackgroundWorker, at line 5696 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that do_start_bgworker passes to BackgroundWorker, at line 5696 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5755	5755
Object	BackgroundWorker	BackgroundWorker

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method do_start_bgworker(RegisteredBgWorker *rw)

```
....
5755.                   memcpy(MyBgworkerEntry, &rw->rw_worker,
sizeof(BackgroundWorker));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=85
Status	New

The size of the buffer used by save_backend_variables in Port, at line 6052 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that save_backend_variables passes to Port, at line 6052 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	6059	6059
Object	Port	Port

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method save_backend_variables(BackendParameters *param, Port *port)

```
....
6059.       memcpy(&param->port, port, sizeof(Port));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=86
Status	New

The size of the buffer used by save_backend_variables in ListenSocket, at line 6052 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that save_backend_variables passes to ListenSocket, at line 6052 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	6065	6065
Object	ListenSocket	ListenSocket

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method save_backend_variables(BackendParameters *param, Port *port)

```
....
6065.       memcpy(&param->ListenSocket, &ListenSocket,
sizeof(ListenSocket));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=87
Status	New

The size of the buffer used by save_backend_variables in syslogPipe, at line 6052 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that save_backend_variables passes to syslogPipe, at line 6052 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	6116	6116
Object	syslogPipe	syslogPipe

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method save_backend_variables(BackendParameters *param, Port *port)

```
....
6116.       memcpy(&param->syslogPipe, &syslogPipe, sizeof(syslogPipe));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=88
Status	New

The size of the buffer used by restore_backend_variables in Port, at line 6294 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that restore_backend_variables passes to Port, at line 6294 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	6296	6296
Object	Port	Port

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method restore_backend_variables(BackendParameters *param, Port *port)

```
....
6296.       memcpy(port, &param->port, sizeof(Port));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=89
Status	New

The size of the buffer used by PQgetCancel in SockAddr, at line 3269 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that PQgetCancel passes to SockAddr, at line 3269 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	3283	3283
Object	SockAddr	SockAddr

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PQgetCancel(PGconn *conn)

```
....
3283.       memcpy(&cancel->raddr, &conn->raddr, sizeof(SockAddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=90
Status	New

The size of the buffer used by set_cmd_start_ms in uint64_t, at line 593 of proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that set_cmd_start_ms passes to uint64_t, at line 593 of proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c, to overwrite the target buffer.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	611	611
Object	uint64_t	uint64_t

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static int set_cmd_start_ms(cmd_rec *cmd) {

```
....
611.    memcpy(v, &start_ms, sizeof(uint64_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=91
Status	New

The size of the buffer used by set_cmd_start_ms in uint64_t, at line 598 of proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that set_cmd_start_ms passes to uint64_t, at line 598 of proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c, to overwrite the target buffer.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	616	616
Object	uint64_t	uint64_t

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static int set_cmd_start_ms(cmd_rec *cmd) {

```
....
616.    memcpy(v, &start_ms, sizeof(uint64_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=92
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2936 of protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2936 of protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Line	2970	2970
Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2970.                          memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=93
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2936 of protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2936 of protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Line	2973	2973
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2973.                          memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=94
Status	New

The size of the buffer used by message_init_generic in protobuf_c_boolean, at line 2943 of protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to protobuf_c_boolean, at line 2943 of protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Line	2977	2977

Object	protobuf_c_boolean	protobuf_c_boolean

Code Snippet
File Name protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2977.                           memcpy(field, dv,
sizeof(protobuf_c_boolean));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=95
Status	New

The size of the buffer used by message_init_generic in ProtobufCBinaryData, at line 2943 of protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that message_init_generic passes to ProtobufCBinaryData, at line 2943 of protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c, to overwrite the target buffer.

	Source	Destination
File	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Line	2980	2980
Object	ProtobufCBinaryData	ProtobufCBinaryData

Code Snippet
File Name protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Method message_init_generic(const ProtobufCMessageDescriptor *desc,

```
....
2980.                           memcpy(field, dv,
sizeof(ProtobufCBinaryData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=96
Status	New

The size of the buffer used by Navigator::fake_traffic in px4_guid_t, at line 956 of PX4@@PX4-Autopilot-v1.11.0-rc1-CVE-2024-30800-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Navigator::fake_traffic passes to px4_guid_t, at line 956 of PX4@@PX4-Autopilot-v1.11.0-rc1-CVE-2024-30800-TP.c, to overwrite the target buffer.

	Source	Destination

File	PX4@@PX4-Autopilot-v1.11.0-rc1-CVE-2024-30800-TP.c	PX4@@PX4-Autopilot-v1.11.0-rc1-CVE-2024-30800-TP.c
Line	995	995
Object	px4_guid_t	px4_guid_t

Code Snippet
File Name PX4@@PX4-Autopilot-v1.11.0-rc1-CVE-2024-30800-TP.c
Method void Navigator::fake_traffic(const char *callsign, float distance, float direction, float traffic_heading,

```
....
995.        memcpy(tr.uas_id, px4_guid, sizeof(px4_guid_t)); //simulate
own GUID
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=97
Status New

The size of the buffer used by Navigator::fake_traffic in px4_guid_t, at line 961 of PX4@@PX4-Autopilot-v1.11.2-CVE-2024-30800-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Navigator::fake_traffic passes to px4_guid_t, at line 961 of PX4@@PX4-Autopilot-v1.11.2-CVE-2024-30800-TP.c, to overwrite the target buffer.

	Source	Destination
File	PX4@@PX4-Autopilot-v1.11.2-CVE-2024-30800-TP.c	PX4@@PX4-Autopilot-v1.11.2-CVE-2024-30800-TP.c
Line	1000	1000
Object	px4_guid_t	px4_guid_t

Code Snippet
File Name PX4@@PX4-Autopilot-v1.11.2-CVE-2024-30800-TP.c
Method void Navigator::fake_traffic(const char *callsign, float distance, float direction, float traffic_heading,

```
....
1000.       memcpy(tr.uas_id, px4_guid, sizeof(px4_guid_t)); //simulate
own GUID
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=98
Status New

The size of the buffer used by Navigator::fake_traffic in px4_guid_t, at line 1039 of PX4@@PX4-Autopilot-v1.12.0-beta1-CVE-2024-30800-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Navigator::fake_traffic passes to px4_guid_t, at line 1039 of PX4@@PX4-Autopilot-v1.12.0-beta1-CVE-2024-30800-TP.c, to overwrite the target buffer.

	Source	Destination
File	PX4@@PX4-Autopilot-v1.12.0-beta1-CVE-2024-30800-TP.c	PX4@@PX4-Autopilot-v1.12.0-beta1-CVE-2024-30800-TP.c
Line	1078	1078
Object	px4_guid_t	px4_guid_t

Code Snippet
File Name PX4@@PX4-Autopilot-v1.12.0-beta1-CVE-2024-30800-TP.c
Method void Navigator::fake_traffic(const char *callsign, float distance, float direction, float traffic_heading,

```
....
1078.       memcpy(tr.uas_id, px4_guid, sizeof(px4_guid_t)); //simulate
own GUID
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=99
Status New

The size of the buffer used by Navigator::fake_traffic in px4_guid_t, at line 1064 of PX4@@PX4-Autopilot-v1.12.0-beta6-CVE-2024-30800-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Navigator::fake_traffic passes to px4_guid_t, at line 1064 of PX4@@PX4-Autopilot-v1.12.0-beta6-CVE-2024-30800-TP.c, to overwrite the target buffer.

	Source	Destination
File	PX4@@PX4-Autopilot-v1.12.0-beta6-CVE-2024-30800-TP.c	PX4@@PX4-Autopilot-v1.12.0-beta6-CVE-2024-30800-TP.c
Line	1103	1103
Object	px4_guid_t	px4_guid_t

Code Snippet
File Name PX4@@PX4-Autopilot-v1.12.0-beta6-CVE-2024-30800-TP.c
Method void Navigator::fake_traffic(const char *callsign, float distance, float direction, float traffic_heading,

```
....
1103.       memcpy(tr.uas_id, px4_guid, sizeof(px4_guid_t)); //simulate
own GUID
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=100
Status	New

The size of the buffer used by Navigator::fake_traffic in px4_guid_t, at line 1131 of PX4@@PX4-Autopilot-v1.13.0-beta1-CVE-2024-30800-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Navigator::fake_traffic passes to px4_guid_t, at line 1131 of PX4@@PX4-Autopilot-v1.13.0-beta1-CVE-2024-30800-TP.c, to overwrite the target buffer.

	Source	Destination
File	PX4@@PX4-Autopilot-v1.13.0-beta1-CVE-2024-30800-TP.c	PX4@@PX4-Autopilot-v1.13.0-beta1-CVE-2024-30800-TP.c
Line	1169	1169
Object	px4_guid_t	px4_guid_t

Code Snippet
File Name PX4@@PX4-Autopilot-v1.13.0-beta1-CVE-2024-30800-TP.c
Method void Navigator::fake_traffic(const char *callsign, float distance, float direction, float traffic_heading,

```
....
1169.       memcpy(tr.uas_id, px4_guid, sizeof(px4_guid_t)); //simulate own GUID
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=101
Status	New

The size of the buffer used by Navigator::fake_traffic in px4_guid_t, at line 1131 of PX4@@PX4-Autopilot-v1.13.1-CVE-2024-30800-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Navigator::fake_traffic passes to px4_guid_t, at line 1131 of PX4@@PX4-Autopilot-v1.13.1-CVE-2024-30800-TP.c, to overwrite the target buffer.

	Source	Destination
File	PX4@@PX4-Autopilot-v1.13.1-CVE-2024-30800-TP.c	PX4@@PX4-Autopilot-v1.13.1-CVE-2024-30800-TP.c
Line	1169	1169
Object	px4_guid_t	px4_guid_t

Code Snippet
File Name PX4@@PX4-Autopilot-v1.13.1-CVE-2024-30800-TP.c
Method void Navigator::fake_traffic(const char *callsign, float distance, float direction, float traffic_heading,

```
....
1169.       memcpy(tr.uas_id, px4_guid, sizeof(px4_guid_t)); //simulate
own GUID
```

Use of Zero Initialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Zero Initialized Pointer Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Zero Initialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2224
Status	New

The variable declared in evi at postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c in line 971 is not initialized when it is used by previous at postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c in line 1101.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	973	1142
Object	evi	previous

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method get_nearest_unprocessed_vertex(List *evi_list)

```
....
973.        ExtensionVersionInfo *evi = NULL;
```

File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c

Method find_update_path(List *evi_list,

```
....
1142.                       evi2->previous = evi;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=2225
Status	New

The variable declared in addrs at postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c in line 1495 is not initialized when it is used by addr_cur at postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c in line 1495.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	1499	1598
Object	addrs	addr_cur

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method connectDBStart(PGconn *conn)

```
....
1499.       struct addrinfo *addrs = NULL;
....
1598.       conn->addr_cur = addrs;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2226
Status	New

The variable declared in addrs at postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c in line 1495 is not initialized when it is used by addrlist at postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c in line 1495.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	1499	1597
Object	addrs	addrlist

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method connectDBStart(PGconn *conn)

```
....
1499.       struct addrinfo *addrs = NULL;
....
1597.       conn->addrlist = addrs;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2227
Status	New

The variable declared in pwd at postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c in line 6028 is not initialized when it is used by pwd at postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c in line 6028.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	6033	6038
Object	pwd	pwd

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method pqGetHomeDirectory(char *buf, int bufsize)

```
....
6033.       struct passwd *pwd = NULL;
....
6038.       strlcpy(buf, pwd->pw_dir, bufsize);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2228
Status	New

The variable declared in addrs at postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c in line 1495 is not initialized when it is used by addr_cur at postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c in line 1495.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	1499	1598
Object	addrs	addr_cur

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method connectDBStart(PGconn *conn)

```
....
1499.       struct addrinfo *addrs = NULL;
....
1598.       conn->addr_cur = addrs;
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2229
Status	New

The variable declared in addrs at postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c in line 1495 is not initialized when it is used by addrlist at postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c in line 1495.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	1499	1597
Object	addrs	addrlist

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method connectDBStart(PGconn *conn)

```
....
1499.       struct addrinfo *addrs = NULL;
....
1597.       conn->addrlist = addrs;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2230
Status	New

The variable declared in pwd at postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c in line 6047 is not initialized when it is used by pwd at postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c in line 6047.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	6052	6057
Object	pwd	pwd

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method pqGetHomeDirectory(char *buf, int bufsize)

```
....
6052.       struct passwd *pwd = NULL;
....
6057.       strlcpy(buf, pwd->pw_dir, bufsize);
```

Use of Zero Initialized Pointer\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2231
Status New

The variable declared in entry_found at projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c in line 62 is not initialized when it is used by entry at projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c in line 390.

	Source	Destination
File	projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c	projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c
Line	67	398
Object	entry_found	entry

Code Snippet
File Name projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c
Method ptirq_lookup_entry_by_sid(uint32_t intr_type,

```
....
67.   struct ptirq_remapping_info *entry_found = NULL;
```

File Name projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c
Method static struct ptirq_remapping_info *add_intx_remapping(struct acrn_vm *vm, uint32_t virt_gsi,

```
....
398.        entry = ptirq_lookup_entry_by_sid(PTDEV_INTR_INTX,
&phys_sid, NULL);
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2232
Status New

The variable declared in entry_found at projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c in line 62 is not initialized when it is used by entry at projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c in line 729.

	Source	Destination
File	projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c	projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c
Line	67	751
Object	entry_found	entry

Code Snippet
File Name projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c
Method ptirq_lookup_entry_by_sid(uint32_t intr_type,

```
....
67.    struct ptirq_remapping_info *entry_found = NULL;
```

File Name projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c
Method int32_t ptirq_intx_pin_remap(struct acrn_vm *vm, uint32_t virt_gsi, enum intx_ctlr vgsi_ctlr)

```
....
751.                entry = ptirq_lookup_entry_by_sid(PTDEV_INTR_INTX,
&virt_sid, vm);
```

Use of Zero Initialized Pointer\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2233
Status New

The variable declared in next at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 159 is not initialized when it is used by next at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 192.

	Source	Destination
File	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Line	162	198
Object	next	next

Code Snippet
File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Method subscription *GetNextSubscription(service_info *service, subscription *current)

```
....
162.      subscription *next = NULL;
```

File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c

Method subscription *GetFirstSubscription(service_info *service)

```
....
198.        next = GetNextSubscription(service, &temp);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2234
Status	New

The variable declared in head at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 729 is not initialized when it is used by head at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 729.

	Source	Destination
File	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Line	831	767
Object	head	head

Code Snippet

File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c

Method service_info *getServiceList(

```
....
831.                                    head = NULL;
....
767.                                head = malloc(sizeof(service_info));
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2235
Status	New

The variable declared in head at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 729 is not initialized when it is used by head at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 729.

	Source	Destination

File	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Line	744	767
Object	head	head

Code Snippet
File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Method service_info *getServiceList(

```
....
744.        service_info *head = NULL;
....
767.                                    head = malloc(sizeof(service_info));
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2236
Status	New

The variable declared in subscriptionList at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 729 is not initialized when it is used by next at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 581.

	Source	Destination
File	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Line	782	602
Object	subscriptionList	next

Code Snippet
File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Method service_info *getServiceList(

```
....
782.                            current->subscriptionList = NULL;
```

File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Method freeServiceList(service_info * head)

```
....
602.          next = head->next;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2237
Status	New

The variable declared in next at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 729 is not initialized when it is used by next at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 581.

	Source	Destination
File	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Line	775	602
Object	next	next

Code Snippet
File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Method service_info *getServiceList(

```
....
775.                            current->next = NULL;
```

File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Method freeServiceList(service_info * head)

```
....
602.            next = head->next;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2238
Status	New

The variable declared in head at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 729 is not initialized when it is used by next at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 862.

	Source	Destination
File	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Line	831	884
Object	head	next

Code Snippet
File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Method service_info *getServiceList(

```
....
831.                                        head = NULL;
```

File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c

Method getAllServiceList(IXML_Node * node,

```
....
884.                            end->next = getServiceList(currentDevice,
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2239
Status	New

The variable declared in head at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 729 is not initialized when it is used by next at pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c in line 862.

	Source	Destination
File	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Line	744	884
Object	head	next

Code Snippet

File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c

Method service_info *getServiceList(

```
....
744.        service_info *head = NULL;
```

File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c

Method getAllServiceList(IXML_Node * node,

```
....
884.                            end->next = getServiceList(currentDevice,
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2240
Status	New

The variable declared in log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1215 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1219	1355
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static struct tlog_log *_tlog_wait_log_locked(struct tlog_log *last_log)

```
....
1219.       struct tlog_log *log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1355.               log = _tlog_wait_log_locked(log);
```

Use of Zero Initialized Pointer\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2241
Status New

The variable declared in log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1327	1347
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1327.       struct tlog_log *log = NULL;
....
1347.           log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2242
Status	New

The variable declared in log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1368	1347
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
....
1347.           log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2243
Status	New

The variable declared in log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1494 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1494.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1496	1504
Object	log	log

Code Snippet

File Name	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method	tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1496.       struct tlog_log *log = NULL;
....
1504.       log = (struct tlog_log *)malloc(sizeof(*log));
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2244
Status	New

The variable declared in log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1215 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1219	1355
Object	log	log

Code Snippet

File Name	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method	static struct tlog_log *_tlog_wait_log_locked(struct tlog_log *last_log)

```
....
1219.       struct tlog_log *log = NULL;
```

File Name	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method	static void *_tlog_work(void *arg)

```
....
1355.               log = _tlog_wait_log_locked(log);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2245
Status	New

The variable declared in log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1327	1347
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1327.      struct tlog_log *log = NULL;
....
1347.          log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2246
Status	New

The variable declared in log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1347
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                      log = NULL;
....
1347.          log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2247
Status	New

The variable declared in log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1494 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1494.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1496	1504
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1496.       struct tlog_log *log = NULL;
....
1504.       log = (struct tlog_log *)malloc(sizeof(*log));
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2248
Status	New

The variable declared in log at pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c in line 1234 is not initialized when it is used by log at pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c in line 1339.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1238	1377
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static struct tlog_log *_tlog_wait_log_locked(struct tlog_log *last_log)

```
....
1238.       struct tlog_log *log = NULL;
```

File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1377.               log = _tlog_wait_log_locked(log);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2249
Status	New

The variable declared in log at pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c in line 1339 is not initialized when it is used by log at pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c in line 1339.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1346	1369
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1346.       struct tlog_log *log = NULL;
....
1369.           log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2250
Status	New

The variable declared in log at pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c in line 1339 is not initialized when it is used by log at pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c in line 1339.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1390	1369
Object	log	log

Code Snippet	
File Name	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method	static void *_tlog_work(void *arg)

```
....
1390.                       log = NULL;
....
1369.          log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2251
Status	New

The variable declared in log at pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c in line 1521 is not initialized when it is used by log at pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c in line 1521.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1523	1531
Object	log	log

Code Snippet	
File Name	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method	tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1523.      struct tlog_log *log = NULL;
....
1531.      log = (struct tlog_log *)malloc(sizeof(*log));
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2252
Status	New

The variable declared in log at pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c in line 1234 is not initialized when it is used by log at pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c in line 1339.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-	pymumu@@smartdns-Release32-RC2-

	CVE-2024-24199-TP.c	CVE-2024-24199-TP.c
Line	1238	1377
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static struct tlog_log *_tlog_wait_log_locked(struct tlog_log *last_log)

```
....
1238.       struct tlog_log *log = NULL;
```

File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1377.               log = _tlog_wait_log_locked(log);
```

Use of Zero Initialized Pointer\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2253
Status New

The variable declared in log at pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c in line 1339 is not initialized when it is used by log at pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c in line 1339.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	1346	1369
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1346.       struct tlog_log *log = NULL;
....
1369.           log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 31:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2254
Status	New

The variable declared in log at pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c in line 1339 is not initialized when it is used by log at pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c in line 1339.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	1390	1369
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1390.                       log = NULL;
....
1369.          log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2255
Status	New

The variable declared in log at pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c in line 1521 is not initialized when it is used by log at pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c in line 1521.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	1523	1531
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1523.       struct tlog_log *log = NULL;
....
1531.       log = (struct tlog_log *)malloc(sizeof(*log));
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2256
Status	New

The variable declared in log at pymumu@@smartdns-Release34-CVE-2024-24198-TP.c in line 1294 is not initialized when it is used by log at pymumu@@smartdns-Release34-CVE-2024-24198-TP.c in line 1398.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1298	1436
Object	log	log

Code Snippet

File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c

Method static struct tlog_log *_tlog_wait_log_locked(struct tlog_log *last_log)

```
....
1298.       struct tlog_log *log = NULL;
```

File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c

Method static void *_tlog_work(void *arg)

```
....
1436.               log = _tlog_wait_log_locked(log);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2257
Status	New

The variable declared in log at pymumu@@smartdns-Release34-CVE-2024-24198-TP.c in line 1398 is not initialized when it is used by log at pymumu@@smartdns-Release34-CVE-2024-24198-TP.c in line 1398.

	Source	Destination

File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1405	1428
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1405.       struct tlog_log *log = NULL;
....
1428.           log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2258
Status	New

The variable declared in log at pymumu@@smartdns-Release34-CVE-2024-24198-TP.c in line 1398 is not initialized when it is used by log at pymumu@@smartdns-Release34-CVE-2024-24198-TP.c in line 1398.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1449	1428
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1449.                       log = NULL;
....
1428.           log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2259
Status	New

The variable declared in log at pymumu@@smartdns-Release34-CVE-2024-24198-TP.c in line 1585 is not initialized when it is used by log at pymumu@@smartdns-Release34-CVE-2024-24198-TP.c in line 1585.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1587	1594
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1587.       struct tlog_log *log = NULL;
....
1594.       log = (struct tlog_log *)malloc(sizeof(*log));
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2260
Status	New

The variable declared in log at pymumu@@smartdns-Release34-CVE-2024-24199-TP.c in line 1294 is not initialized when it is used by log at pymumu@@smartdns-Release34-CVE-2024-24199-TP.c in line 1398.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1298	1436
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static struct tlog_log *_tlog_wait_log_locked(struct tlog_log *last_log)

```
....
1298.       struct tlog_log *log = NULL;
```

File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1436.               log = _tlog_wait_log_locked(log);
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2261
Status	New

The variable declared in log at pymumu@@smartdns-Release34-CVE-2024-24199-TP.c in line 1398 is not initialized when it is used by log at pymumu@@smartdns-Release34-CVE-2024-24199-TP.c in line 1398.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1405	1428
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1405.      struct tlog_log *log = NULL;
....
1428.          log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2262
Status	New

The variable declared in log at pymumu@@smartdns-Release34-CVE-2024-24199-TP.c in line 1398 is not initialized when it is used by log at pymumu@@smartdns-Release34-CVE-2024-24199-TP.c in line 1398.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1449	1428
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1449.                      log = NULL;
....
1428.          log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2263
Status	New

The variable declared in log at pymumu@@smartdns-Release34-CVE-2024-24199-TP.c in line 1585 is not initialized when it is used by log at pymumu@@smartdns-Release34-CVE-2024-24199-TP.c in line 1585.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1587	1594
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1587.       struct tlog_log *log = NULL;
....
1594.       log = (struct tlog_log *)malloc(sizeof(*log));
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2264
Status	New

The variable declared in log at pymumu@@smartdns-Release36-CVE-2024-24198-TP.c in line 1294 is not initialized when it is used by log at pymumu@@smartdns-Release36-CVE-2024-24198-TP.c in line 1427.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1298	1468
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static struct tlog_log *_tlog_wait_log_locked(struct tlog_log *last_log)

```
....
1298.       struct tlog_log *log = NULL;
```

File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c

Method static void *_tlog_work(void *arg)

```
....
1468.               log = _tlog_wait_log_locked(log);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2265
Status	New

The variable declared in log at pymumu@@smartdns-Release36-CVE-2024-24198-TP.c in line 1427 is not initialized when it is used by log at pymumu@@smartdns-Release36-CVE-2024-24198-TP.c in line 1427.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1434	1460
Object	log	log

Code Snippet

File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c

Method static void *_tlog_work(void *arg)

```
....
1434.       struct tlog_log *log = NULL;
....
1460.           log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2266
Status	New

The variable declared in log at pymumu@@smartdns-Release36-CVE-2024-24198-TP.c in line 1427 is not initialized when it is used by log at pymumu@@smartdns-Release36-CVE-2024-24198-TP.c in line 1427.

	Source	Destination

File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1481	1460
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1481.                       log = NULL;
....
1460.           log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2267
Status	New

The variable declared in log at pymumu@@smartdns-Release36-CVE-2024-24198-TP.c in line 1617 is not initialized when it is used by log at pymumu@@smartdns-Release36-CVE-2024-24198-TP.c in line 1617.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1619	1626
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1619.       struct tlog_log *log = NULL;
....
1626.       log = (struct tlog_log *)malloc(sizeof(*log));
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2268
Status	New

The variable declared in log at pymumu@@smartdns-Release36-CVE-2024-24199-TP.c in line 1294 is not initialized when it is used by log at pymumu@@smartdns-Release36-CVE-2024-24199-TP.c in line 1427.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	1298	1468
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static struct tlog_log *_tlog_wait_log_locked(struct tlog_log *last_log)

```
....
1298.       struct tlog_log *log = NULL;
```

File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1468.               log = _tlog_wait_log_locked(log);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2269
Status	New

The variable declared in log at pymumu@@smartdns-Release36-CVE-2024-24199-TP.c in line 1427 is not initialized when it is used by log at pymumu@@smartdns-Release36-CVE-2024-24199-TP.c in line 1427.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	1434	1460
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1434.       struct tlog_log *log = NULL;
....
1460.           log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2270
Status	New

The variable declared in log at pymumu@@smartdns-Release36-CVE-2024-24199-TP.c in line 1427 is not initialized when it is used by log at pymumu@@smartdns-Release36-CVE-2024-24199-TP.c in line 1427.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	1481	1460
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1481.                       log = NULL;
....
1460.          log = _tlog_next_log(log);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2271
Status	New

The variable declared in log at pymumu@@smartdns-Release36-CVE-2024-24199-TP.c in line 1617 is not initialized when it is used by log at pymumu@@smartdns-Release36-CVE-2024-24199-TP.c in line 1617.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	1619	1626
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1619.       struct tlog_log *log = NULL;
....
1626.       log = (struct tlog_log *)malloc(sizeof(*log));
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2272
Status	New

The variable declared in log at pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c in line 1326 is not initialized when it is used by log at pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c in line 1459.

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	1330	1500
Object	log	log

Code Snippet

File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c

Method static struct tlog_log *_tlog_wait_log_locked(struct tlog_log *last_log)

```
....
1330.       struct tlog_log *log = NULL;
```

File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c

Method static void *_tlog_work(void *arg)

```
....
1500.               log = _tlog_wait_log_locked(log);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2273
Status	New

The variable declared in log at pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c in line 1459 is not initialized when it is used by log at pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c in line 1459.

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	1466	1492
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1466.       struct tlog_log *log = NULL;
....
1492.           log = _tlog_next_log(log);
```

Memory Leak

Query Path:
CPP\Cx\CPP Medium Threat\Memory Leak Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Memory Leak\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2047
Status New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Line	193	193
Object	value	value

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
193.                tuple->value = pkgconf_tuple_parse(client, list,
dequote_value);
```

Memory Leak\Path 2:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2048
Status	New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Line	193	193
Object	value	value

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
193.                tuple->value = pkgconf_tuple_parse(client, list,
dequote_value);
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2049
Status	New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Line	193	193
Object	value	value

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
193.                tuple->value = pkgconf_tuple_parse(client, list,
dequote_value);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2050

Status	New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Line	230	230
Object	value	value

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse, unsigned int flags)

```
....
230.              tuple->value = pkgconf_tuple_parse(client, list,
dequote_value, flags);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2051
Status	New

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-0520-FP.c	python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Line	705	705
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet
File Name python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method tracemalloc_malloc_gil(void *ctx, size_t size)

```
....
705.      return tracemalloc_alloc_gil(0, ctx, 1, size);
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2052
Status	New

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-	python@@cpython-v3.10.0-CVE-2022-

	0520-FP.c	0520-FP.c
Line	712	712
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet
File Name python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method tracemalloc_calloc_gil(void *ctx, size_t nelem, size_t elsize)

```
....
712.      return tracemalloc_alloc_gil(1, ctx, nelem, elsize);
```

Memory Leak\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2053
Status New

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-0520-FP.c	python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Line	781	781
Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method tracemalloc_raw_malloc(void *ctx, size_t size)

```
....
781.      return tracemalloc_raw_alloc(0, ctx, 1, size);
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2054
Status New

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-0520-FP.c	python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Line	788	788
Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet

File Name	python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method	tracemalloc_raw_calloc(void *ctx, size_t nelem, size_t elsize)

```
....
788.      return tracemalloc_raw_alloc(1, ctx, nelem, elsize);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2055
Status	New

	Source	Destination
File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	705	705
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet

File Name	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method	tracemalloc_malloc_gil(void *ctx, size_t size)

```
....
705.      return tracemalloc_alloc_gil(0, ctx, 1, size);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2056
Status	New

	Source	Destination
File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	712	712
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet

File Name	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method	tracemalloc_calloc_gil(void *ctx, size_t nelem, size_t elsize)

```
....
712.      return tracemalloc_alloc_gil(1, ctx, nelem, elsize);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2057
Status	New

	Source	Destination
File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	781	781
Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method tracemalloc_raw_malloc(void *ctx, size_t size)

```
....
781.      return tracemalloc_raw_alloc(0, ctx, 1, size);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2058
Status	New

	Source	Destination
File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	788	788
Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method tracemalloc_raw_calloc(void *ctx, size_t nelem, size_t elsize)

```
....
788.      return tracemalloc_raw_alloc(1, ctx, nelem, elsize);
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2059
Status	New

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	705	705
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet
File Name python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Method tracemalloc_malloc_gil(void *ctx, size_t size)

```
....
705.      return tracemalloc_alloc_gil(0, ctx, 1, size);
```

Memory Leak\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2060
Status New

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	712	712
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet
File Name python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Method tracemalloc_calloc_gil(void *ctx, size_t nelem, size_t elsize)

```
....
712.      return tracemalloc_alloc_gil(1, ctx, nelem, elsize);
```

Memory Leak\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2061
Status New

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	781	781

Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Method tracemalloc_raw_malloc(void *ctx, size_t size)

```
....
781.      return tracemalloc_raw_alloc(0, ctx, 1, size);
```

Memory Leak\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2062
Status New

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	788	788
Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Method tracemalloc_raw_calloc(void *ctx, size_t nelem, size_t elsize)

```
....
788.      return tracemalloc_raw_alloc(1, ctx, nelem, elsize);
```

Memory Leak\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2063
Status New

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	705	705
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet
File Name python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method tracemalloc_malloc_gil(void *ctx, size_t size)

```
....
705.      return tracemalloc_alloc_gil(0, ctx, 1, size);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2064
Status	New

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	712	712
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet
File Name python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method tracemalloc_calloc_gil(void *ctx, size_t nelem, size_t elsize)

```
....
712.      return tracemalloc_alloc_gil(1, ctx, nelem, elsize);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2065
Status	New

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	781	781
Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method tracemalloc_raw_malloc(void *ctx, size_t size)

```
....
781.      return tracemalloc_raw_alloc(0, ctx, 1, size);
```

Memory Leak\Path 20:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2066
Status	New

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	788	788
Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method tracemalloc_raw_calloc(void *ctx, size_t nelem, size_t elsize)

```
....
788.      return tracemalloc_raw_alloc(1, ctx, nelem, elsize);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2067
Status	New

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	705	705
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet
File Name python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method tracemalloc_malloc_gil(void *ctx, size_t size)

```
....
705.      return tracemalloc_alloc_gil(0, ctx, 1, size);
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2068
Status	New

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	712	712
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet
File Name python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method tracemalloc_calloc_gil(void *ctx, size_t nelem, size_t elsize)

```
....
712.      return tracemalloc_alloc_gil(1, ctx, nelem, elsize);
```

Memory Leak\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2069
Status New

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	781	781
Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method tracemalloc_raw_malloc(void *ctx, size_t size)

```
....
781.      return tracemalloc_raw_alloc(0, ctx, 1, size);
```

Memory Leak\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2070
Status New

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	788	788

Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method tracemalloc_raw_calloc(void *ctx, size_t nelem, size_t elsize)

```
....
788.      return tracemalloc_raw_alloc(1, ctx, nelem, elsize);
```

Memory Leak\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2071
Status New

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Line	705	705
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method tracemalloc_malloc_gil(void *ctx, size_t size)

```
....
705.      return tracemalloc_alloc_gil(0, ctx, 1, size);
```

Memory Leak\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2072
Status New

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Line	712	712
Object	tracemalloc_alloc_gil	tracemalloc_alloc_gil

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method tracemalloc_calloc_gil(void *ctx, size_t nelem, size_t elsize)

```
....
712.      return tracemalloc_alloc_gil(1, ctx, nelem, elsize);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2073
Status	New

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Line	781	781
Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method tracemalloc_raw_malloc(void *ctx, size_t size)

```
....
781.      return tracemalloc_raw_alloc(0, ctx, 1, size);
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2074
Status	New

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Line	788	788
Object	tracemalloc_raw_alloc	tracemalloc_raw_alloc

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method tracemalloc_raw_calloc(void *ctx, size_t nelem, size_t elsize)

```
....
788.      return tracemalloc_raw_alloc(1, ctx, nelem, elsize);
```

Memory Leak\Path 29:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2075
Status	New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Line	183	183
Object	tuple	tuple

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
183.        pkgconf_tuple_t *tuple = calloc(sizeof(pkgconf_tuple_t), 1);
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2076
Status	New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Line	183	183
Object	tuple	tuple

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
183.        pkgconf_tuple_t *tuple = calloc(sizeof(pkgconf_tuple_t), 1);
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2077
Status	New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Line	183	183
Object	tuple	tuple

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
183.        pkgconf_tuple_t *tuple = calloc(sizeof(pkgconf_tuple_t), 1);
```

Memory Leak\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2078
Status New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Line	222	222
Object	tuple	tuple

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse, unsigned int flags)

```
....
222.        pkgconf_tuple_t *tuple = calloc(sizeof(pkgconf_tuple_t), 1);
```

Memory Leak\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2079
Status New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c

Line	191	191
Object	key	key

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
191.        tuple->key = strdup(key);
```

Memory Leak\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2080
Status New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Line	195	195
Object	value	value

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
195.              tuple->value = strdup(dequote_value);
```

Memory Leak\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2081
Status New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Line	191	191
Object	key	key

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
191.        tuple->key = strdup(key);
```

Memory Leak\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2082
Status New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Line	195	195
Object	value	value

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
195.              tuple->value = strdup(dequote_value);
```

Memory Leak\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2083
Status New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Line	191	191
Object	key	key

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
191.        tuple->key = strdup(key);
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2084
Status	New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Line	195	195
Object	value	value

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse)

```
....
195.              tuple->value = strdup(dequote_value);
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2085
Status	New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Line	228	228
Object	key	key

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse, unsigned int flags)

```
....
228.        tuple->key = strdup(key);
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2086
Status	New

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Line	232	232
Object	value	value

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_add(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key, const char *value, bool parse, unsigned int flags)

```
....
232.              tuple->value = strdup(dequote_value);
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2087
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	679	679
Object	output_config_variable	output_config_variable

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
679.                          output_config_variable = strdup(optarg);
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2088

Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	683	683
Object	userDoption	userDoption

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
683.                            userDoption = strdup(optarg);
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2089
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	2408	2408
Object	port	port

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method ConnCreate(int serverFd)

```
....
2408.       if (!(port = (Port *) calloc(1, sizeof(Port))))
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2090
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c

Line	2438	2438
Object	gss	gss

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method ConnCreate(int serverFd)

```
....
2438.       port->gss = (pg_gssinfo *) calloc(1, sizeof(pg_gssinfo));
```

Memory Leak\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2091
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4181	4181
Object	remote_host	remote_host

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method BackendInitialize(Port *port)

```
....
4181.       port->remote_host = strdup(remote_host);
```

Memory Leak\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2092
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4182	4182
Object	remote_port	remote_port

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c

Method	BackendInitialize(Port *port)

```
....
4182.       port->remote_port = strdup(remote_port);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2093
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4213	4213
Object	remote_hostname	remote_hostname

Code Snippet	
File Name	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method	BackendInitialize(Port *port)

```
....
4213.             port->remote_hostname = strdup(remote_host);
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2094
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4742	4742
Object	gss	gss

Code Snippet	
File Name	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method	SubPostmasterMain(int argc, char *argv[])

```
....
4742.       port.gss = (pg_gssinfo *) calloc(1, sizeof(pg_gssinfo));
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2095
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5770	5770
Object	bn	bn

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method assign_backendlist_entry(RegisteredBgWorker *rw)

```
....
5770.       bn = malloc(sizeof(Backend));
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2096
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	912	912
Object	dbName	dbName

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method connectOptions2(PGconn *conn)

```
....
912.              conn->dbName = strdup(conn->pguser);
```

Wrong Size t Allocation

Query Path:
CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0

Description

Wrong Size t Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=443
Status	New

The function size in python@@cpython-v3.10.0-CVE-2022-0520-FP.c at line 252 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-0520-FP.c	python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Line	254	254
Object	size	size

Code Snippet
File Name python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method raw_malloc(size_t size)

```
....
254.        return allocators.raw.malloc(allocators.raw.ctx, size);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=444
Status	New

The function size in python@@cpython-v3.10.11-CVE-2022-0520-FP.c at line 252 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	254	254
Object	size	size

Code Snippet
File Name python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method raw_malloc(size_t size)

```
....
254.        return allocators.raw.malloc(allocators.raw.ctx, size);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=445
Status	New

The function size in python@@cpython-v3.10.7-CVE-2022-0520-FP.c at line 252 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	254	254
Object	size	size

Code Snippet
File Name python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Method raw_malloc(size_t size)

```
....
254.      return allocators.raw.malloc(allocators.raw.ctx, size);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=446
Status	New

The function size in python@@cpython-v3.9.13-CVE-2022-0520-FP.c at line 252 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	254	254
Object	size	size

Code Snippet
File Name python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method raw_malloc(size_t size)

```
....
254.      return allocators.raw.malloc(allocators.raw.ctx, size);
```

Wrong Size t Allocation\Path 5:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=447
Status	New

The function size in python@@cpython-v3.9.16-CVE-2022-0520-FP.c at line 252 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	254	254
Object	size	size

Code Snippet
File Name python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method raw_malloc(size_t size)

```
....
254.      return allocators.raw.malloc(allocators.raw.ctx, size);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=448
Status	New

The function size in python@@cpython-v3.9.6-CVE-2022-0520-FP.c at line 252 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Line	254	254
Object	size	size

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method raw_malloc(size_t size)

```
....
254.      return allocators.raw.malloc(allocators.raw.ctx, size);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=449
Status	New

The function elsize in python@@cpython-v3.10.0-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-0520-FP.c	python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Line	589	589
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
589.          ptr = alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=450
Status	New

The function elsize in python@@cpython-v3.10.0-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-0520-FP.c	python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Line	685	685
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
685.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=451
Status	New

The function elsize in python@@cpython-v3.10.0-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-0520-FP.c	python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Line	759	759
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
759.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=452
Status	New

The function elsize in python@@cpython-v3.10.11-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	589	589
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
589.          ptr = alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=453
Status	New

The function elsize in python@@cpython-v3.10.11-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	685	685
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
685.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=454
Status	New

The function elsize in python@@cpython-v3.10.11-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	759	759
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
759.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=455
Status	New

The function elsize in python@@cpython-v3.10.7-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	589	589
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Method tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
589.          ptr = alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=456
Status	New

The function elsize in python@@cpython-v3.10.7-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	685	685
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.7-CVE-2022-0520-FP.c

Method	tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
685.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=457
Status	New

The function elsize in python@@cpython-v3.10.7-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	759	759
Object	elsize	elsize

Code Snippet	
File Name	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Method	tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
759.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=458
Status	New

The function elsize in python@@cpython-v3.9.13-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	589	589
Object	elsize	elsize

Code Snippet

File Name	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method	tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
589.          ptr = alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=459
Status	New

The function elsize in python@@cpython-v3.9.13-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	685	685
Object	elsize	elsize

Code Snippet

File Name	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method	tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
685.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=460
Status	New

The function elsize in python@@cpython-v3.9.13-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	759	759
Object	elsize	elsize

Code Snippet	
File Name	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method	tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
759.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=461
Status	New

The function elsize in python@@cpython-v3.9.16-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	589	589
Object	elsize	elsize

Code Snippet	
File Name	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method	tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
589.          ptr = alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=462
Status	New

The function elsize in python@@cpython-v3.9.16-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	685	685
Object	elsize	elsize

Code Snippet	
File Name	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method	tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
685.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=463
Status	New

The function elsize in python@@cpython-v3.9.16-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	759	759
Object	elsize	elsize

Code Snippet	
File Name	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method	tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
759.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=464
Status	New

The function elsize in python@@cpython-v3.9.6-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Line	589	589

Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
589.          ptr = alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=465
Status New

The function elsize in python@@cpython-v3.9.6-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Line	685	685
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
685.              return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=466
Status New

The function elsize in python@@cpython-v3.9.6-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c

Line	759	759
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
759.             return alloc->calloc(alloc->ctx, nelem, elsize);
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=467
Status	New

The function elsize in python@@cpython-v3.10.0-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-0520-FP.c	python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Line	591	591
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
591.         ptr = alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=468
Status	New

The function elsize in python@@cpython-v3.10.0-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-	python@@cpython-v3.10.0-CVE-2022-

	0520-FP.c	0520-FP.c
Line	687	687
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
687.                return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=469
Status New

The function elsize in python@@cpython-v3.10.0-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.0-CVE-2022-0520-FP.c	python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Line	761	761
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.0-CVE-2022-0520-FP.c
Method tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
761.                return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=470
Status New

The function elsize in python@@cpython-v3.10.11-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination

File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	591	591
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
591.          ptr = alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=471
Status New

The function elsize in python@@cpython-v3.10.11-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	687	687
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
687.              return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=472
Status New

The function elsize in python@@cpython-v3.10.11-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.11-CVE-2022-0520-FP.c	python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Line	761	761
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.11-CVE-2022-0520-FP.c
Method tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
761.              return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=473
Status New

The function elsize in python@@cpython-v3.10.7-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	591	591
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Method tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
591.          ptr = alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=474
Status New

The function elsize in python@@cpython-v3.10.7-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	687	687
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Method tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
687.                return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=475
Status New

The function elsize in python@@cpython-v3.10.7-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.10.7-CVE-2022-0520-FP.c	python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Line	761	761
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.10.7-CVE-2022-0520-FP.c
Method tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
761.                return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=476
Status New

The function elsize in python@@cpython-v3.9.13-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	591	591
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
591.          ptr = alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=477
Status New

The function elsize in python@@cpython-v3.9.13-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	687	687
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
687.              return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=478
Status New

The function elsize in python@@cpython-v3.9.13-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.13-CVE-2022-0520-FP.c	python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Line	761	761
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.13-CVE-2022-0520-FP.c
Method tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
761.              return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=479
Status New

The function elsize in python@@cpython-v3.9.16-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	591	591
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
591.          ptr = alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=480
Status New

The function elsize in python@@cpython-v3.9.16-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	687	687
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
687.                return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=481
Status New

The function elsize in python@@cpython-v3.9.16-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.16-CVE-2022-0520-FP.c	python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Line	761	761
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.16-CVE-2022-0520-FP.c
Method tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
761.                return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=482
Status New

The function elsize in python@@cpython-v3.9.6-CVE-2022-0520-FP.c at line 581 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Line	591	591
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method tracemalloc_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
591.          ptr = alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=483
Status New

The function elsize in python@@cpython-v3.9.6-CVE-2022-0520-FP.c at line 678 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Line	687	687
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method tracemalloc_alloc_gil(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
687.              return alloc->malloc(alloc->ctx, nelem * elsize);
```

Wrong Size t Allocation\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=484
Status New

The function elsize in python@@cpython-v3.9.6-CVE-2022-0520-FP.c at line 751 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	python@@cpython-v3.9.6-CVE-2022-0520-FP.c	python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Line	761	761
Object	elsize	elsize

Code Snippet
File Name python@@cpython-v3.9.6-CVE-2022-0520-FP.c
Method tracemalloc_raw_alloc(int use_calloc, void *ctx, size_t nelem, size_t elsize)

```
....
761.              return alloc->malloc(alloc->ctx, nelem * elsize);
```

MemoryFree on StackVariable

Query Path:
CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=399
Status	New

Calling free() (line 771) on a variable that was not dynamically allocated (line 771) in file postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	809	809
Object	varname	varname

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
809.                          free(varname);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=400
Status	New

Calling free() (line 771) on a variable that was not dynamically allocated (line 771) in file postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	814	814
Object	varname	varname

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
814.                    free(varname);
```

MemoryFree on StackVariable\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=401
Status New

Calling free() (line 2061) on a variable that was not dynamically allocated (line 2061) in file postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	2103	2103
Object	fn	fn

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method expand_tilde(char **filename)

```
....
2103.                   free(fn);
```

MemoryFree on StackVariable\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=402
Status New

Calling free() (line 566) on a variable that was not dynamically allocated (line 566) in file postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	824	824
Object	name	name

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
824.                                    free(name);
```

MemoryFree on StackVariable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=403
Status New

Calling free() (line 566) on a variable that was not dynamically allocated (line 566) in file postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	826	826
Object	value	value

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
826.                                        free(value);
```

MemoryFree on StackVariable\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=404
Status New

Calling free() (line 3197) on a variable that was not dynamically allocated (line 3197) in file postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	3267	3267
Object	bp	bp

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method CleanupBackend(int pid,

```
....
3267.                   free(bp);
```

MemoryFree on StackVariable\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=405
Status New

Calling free() (line 3281) on a variable that was not dynamically allocated (line 3281) in file postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	3370	3370
Object	bp	bp

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method HandleChildCrash(int pid, int exitstatus, const char *procname)

```
....
3370.                   free(bp);
```

MemoryFree on StackVariable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=406
Status New

Calling free() (line 6349) on a variable that was not dynamically allocated (line 6349) in file postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	6386	6386
Object	childinfo	childinfo

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method pgwin32_deadchild_callback(PVOID lpParameter, BOOLEAN TimerOrWaitFired)

```
....
6386.        free(childinfo);
```

MemoryFree on StackVariable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=407
Status New

Calling free() (line 487) on a variable that was not dynamically allocated (line 487) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	499	499
Object	prev	prev

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method pqDropServerData(PGconn *conn)

```
....
499.                free(prev);
```

MemoryFree on StackVariable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=408
Status New

Calling free() (line 487) on a variable that was not dynamically allocated (line 487) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	510	510
Object	prev	prev

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method pqDropServerData(PGconn *conn)

```
....
510.                free(prev);
```

MemoryFree on StackVariable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=409
Status New

Calling free() (line 1738) on a variable that was not dynamically allocated (line 1738) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	2268	2268
Object	startpacket	startpacket

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
2268.                                   free(startpacket);
```

MemoryFree on StackVariable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=410
Status New

Calling free() (line 1738) on a variable that was not dynamically allocated (line 1738) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	2272	2272
Object	startpacket	startpacket

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
2272.                           free(startpacket);
```

MemoryFree on StackVariable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=411
Status New

Calling free() (line 5070) on a variable that was not dynamically allocated (line 5070) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5134	5134
Object	keyword	keyword

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5134.                       free(keyword);
```

MemoryFree on StackVariable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=412
Status New

Calling free() (line 5070) on a variable that was not dynamically allocated (line 5070) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5145	5145
Object	keyword	keyword

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5145.                    free(keyword);
```

MemoryFree on StackVariable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=413
Status New

Calling free() (line 5070) on a variable that was not dynamically allocated (line 5070) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5146	5146
Object	value	value

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5146.                    free(value);
```

MemoryFree on StackVariable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=414
Status New

Calling free() (line 5070) on a variable that was not dynamically allocated (line 5070) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5169	5169
Object	keyword	keyword

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5169.                           free(keyword);
```

MemoryFree on StackVariable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=415
Status New

Calling free() (line 5070) on a variable that was not dynamically allocated (line 5070) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5170	5170
Object	value	value

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5170.                           free(value);
```

MemoryFree on StackVariable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=416
Status New

Calling free() (line 5070) on a variable that was not dynamically allocated (line 5070) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5177	5177
Object	keyword	keyword

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5177.                    free(keyword);
```

MemoryFree on StackVariable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=417
Status New

Calling free() (line 5070) on a variable that was not dynamically allocated (line 5070) in file postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5178	5178
Object	value	value

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5178.                    free(value);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=418
Status New

Calling free() (line 578) on a variable that was not dynamically allocated (line 578) in file postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	843	843
Object	name	name

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
843.                                    free(name);
```

MemoryFree on StackVariable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=419
Status New

Calling free() (line 578) on a variable that was not dynamically allocated (line 578) in file postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	845	845
Object	value	value

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
845.                                    free(value);
```

MemoryFree on StackVariable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=420
Status New

Calling free() (line 3209) on a variable that was not dynamically allocated (line 3209) in file postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	3279	3279
Object	bp	bp

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method CleanupBackend(int pid,

```
....
3279.                    free(bp);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=421
Status New

Calling free() (line 3293) on a variable that was not dynamically allocated (line 3293) in file postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	3382	3382
Object	bp	bp

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method HandleChildCrash(int pid, int exitstatus, const char *procname)

```
....
3382.                    free(bp);
```

MemoryFree on StackVariable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=422
Status New

Calling free() (line 6427) on a variable that was not dynamically allocated (line 6427) in file postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	6464	6464
Object	childinfo	childinfo

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method pgwin32_deadchild_callback(PVOID lpParameter, BOOLEAN TimerOrWaitFired)

```
....
6464.        free(childinfo);
```

MemoryFree on StackVariable\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=423
Status New

Calling free() (line 487) on a variable that was not dynamically allocated (line 487) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	499	499
Object	prev	prev

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method pqDropServerData(PGconn *conn)

```
....
499.                free(prev);
```

MemoryFree on StackVariable\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=424
Status New

Calling free() (line 487) on a variable that was not dynamically allocated (line 487) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	510	510
Object	prev	prev

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method pqDropServerData(PGconn *conn)

```
....
510.                free(prev);
```

MemoryFree on StackVariable\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=425
Status New

Calling free() (line 1738) on a variable that was not dynamically allocated (line 1738) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	2268	2268
Object	startpacket	startpacket

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
2268.                                   free(startpacket);
```

MemoryFree on StackVariable\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=426
Status New

Calling free() (line 1738) on a variable that was not dynamically allocated (line 1738) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	2272	2272
Object	startpacket	startpacket

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
2272.                           free(startpacket);
```

MemoryFree on StackVariable\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=427
Status New

Calling free() (line 5073) on a variable that was not dynamically allocated (line 5073) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5137	5137
Object	keyword	keyword

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5137.                       free(keyword);
```

MemoryFree on StackVariable\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=428
Status New

Calling free() (line 5073) on a variable that was not dynamically allocated (line 5073) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5148	5148
Object	keyword	keyword

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5148.                    free(keyword);
```

MemoryFree on StackVariable\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=429
Status New

Calling free() (line 5073) on a variable that was not dynamically allocated (line 5073) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5149	5149
Object	value	value

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5149.                    free(value);
```

MemoryFree on StackVariable\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=430
Status New

Calling free() (line 5073) on a variable that was not dynamically allocated (line 5073) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5172	5172
Object	keyword	keyword

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5172.                           free(keyword);
```

MemoryFree on StackVariable\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=431
Status New

Calling free() (line 5073) on a variable that was not dynamically allocated (line 5073) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5173	5173
Object	value	value

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5173.                           free(value);
```

MemoryFree on StackVariable\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=432
Status New

Calling free() (line 5073) on a variable that was not dynamically allocated (line 5073) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5180	5180
Object	keyword	keyword

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5180.                    free(keyword);
```

MemoryFree on StackVariable\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=433
Status New

Calling free() (line 5073) on a variable that was not dynamically allocated (line 5073) in file postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c may result with a crash.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5181	5181
Object	value	value

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method conninfo_uri_parse_params(char *params,

```
....
5181.                    free(value);
```

MemoryFree on StackVariable\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=434
Status New

Calling free() (line 2052) on a variable that was not dynamically allocated (line 2052) in file proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c may result with a crash.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	2089	2089
Object	line	line

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void show_os_release(void) {

```
....
2089.       free(line);
```

Double Free

Query Path:
CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description

Double Free\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2024
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	809	814
Object	varname	varname

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method StoreQueryTuple(const PGresult *result)

```
....
809.                            free(varname);
....
814.                        free(varname);
```

Double Free\Path 2:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2025
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	2268	2272
Object	startpacket	startpacket

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
2268.                                   free(startpacket);
....
2272.                               free(startpacket);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2026
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	2268	2272
Object	startpacket	startpacket

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
2268.                                   free(startpacket);
....
2272.                               free(startpacket);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2027

Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1187	1187
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1187.           free(log);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2028
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1187	1187
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1187.           free(log);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2029
Status	New

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c

Line	1206	1206
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1206.           free(log);
```

Double Free\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2030
Status New

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	1206	1206
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1206.           free(log);
```

Double Free\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2031
Status New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1266	1266
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c

Method	static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1266.           free(log);
```

Double Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2032
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1266	1266
Object	log	log

Code Snippet

File Name	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method	static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1266.           free(log);
```

Double Free\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2033
Status	New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1266	1266
Object	log	log

Code Snippet

File Name	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method	static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1266.           free(log);
```

Double Free\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2034
Status	New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	1266	1266
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1266.           free(log);
```

Double Free\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2035
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	1298	1298
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1298.           free(log);
```

Double Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2036
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	1298	1298
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1298.           free(log);
```

Double Free\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2037
Status New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	1310	1310
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1310.           free(log);
```

Double Free\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2038
Status New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Line	1310	1310

Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1310.           free(log);
```

Double Free\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2039
Status New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Line	1333	1333
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1333.           free(log);
```

Double Free\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2040
Status New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Line	1333	1333
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1333.           free(log);
```

Double Free\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2041
Status	New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Line	1348	1348
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1348.           free(log);
```

Double Free\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2042
Status	New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Line	1348	1348
Object	log	log

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Method static int _tlog_close(struct tlog_log *log, int wait_hang)

```
....
1348.           free(log);
```

Use of Uninitialized Pointer

Query Path:

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2201
Status	New

The variable declared in environ at postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c in line 566 is not initialized when it is used by environ at postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c in line 566.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	917	925
Object	environ	environ

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
917.                extern char **environ;
....
925.                for (p = environ; *p; ++p)
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2202
Status	New

The variable declared in environ at postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c in line 578 is not initialized when it is used by environ at postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c in line 578.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	936	944
Object	environ	environ

Code Snippet	
File Name	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method	PostmasterMain(int argc, char *argv[])

```
....
936.              extern char **environ;
....
944.              for (p = environ; *p; ++p)
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2203
Status	New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c in line 64 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c in line 64.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Line	66	70
Object	node	data

Code Snippet	
File Name	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Method	pkgconf_tuple_find_global(const pkgconf_client_t *client, const char *key)

```
....
66.   pkgconf_node_t *node;
....
70.         pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2204
Status	New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c in line 123 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c in line 123.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Line	125	129

Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Method pkgconf_tuple_find_delete(pkgconf_list_t *list, const char *key)

```
....
125.        pkgconf_node_t *node, *next;
....
129.              pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2205
Status New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c in line 218 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c in line 218.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Line	220	228
Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Method pkgconf_tuple_find(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key)

```
....
220.        pkgconf_node_t *node;
....
228.              pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2206
Status New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c in line 64 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c in line 64.

	Source	Destination

File	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Line	66	70
Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Method pkgconf_tuple_find_global(const pkgconf_client_t *client, const char *key)

```
....
66.   pkgconf_node_t *node;
....
70.         pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2207
Status	New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c in line 123 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c in line 123.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Line	125	129
Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Method pkgconf_tuple_find_delete(pkgconf_list_t *list, const char *key)

```
....
125.        pkgconf_node_t *node, *next;
....
129.              pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2208
Status	New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c in line 218 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c in line 218.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Line	220	228
Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Method pkgconf_tuple_find(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key)

```
....
220.        pkgconf_node_t *node;
....
228.              pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2209
Status New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c in line 64 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c in line 64.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Line	66	70
Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_find_global(const pkgconf_client_t *client, const char *key)

```
....
66.   pkgconf_node_t *node;
....
70.         pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2210
Status New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c in line 123 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c in line 123.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Line	125	129
Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_find_delete(pkgconf_list_t *list, const char *key)

```
....
125.        pkgconf_node_t *node, *next;
....
129.              pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2211
Status New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c in line 218 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c in line 218.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Line	220	228
Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_find(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key)

```
....
220.        pkgconf_node_t *node;
....
228.              pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=2212
Status	New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c in line 64 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c in line 64.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Line	66	70
Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_find_global(const pkgconf_client_t *client, const char *key)

```
....
66.   pkgconf_node_t *node;
....
70.         pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2213
Status	New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c in line 123 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c in line 123.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Line	125	129
Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_find_delete(pkgconf_list_t *list, const char *key)

```
....
125.        pkgconf_node_t *node, *next;
....
129.              pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 14:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2214
Status	New

The variable declared in node at pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c in line 257 is not initialized when it is used by data at pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c in line 257.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Line	259	263
Object	node	data

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_find(const pkgconf_client_t *client, pkgconf_list_t *list, const char *key)

```
....
259.        pkgconf_node_t *node;
....
263.              pkgconf_tuple_t *tuple = node->data;
```

Use of Uninitialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2215
Status	New

The variable declared in arr at podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c in line 61 is not initialized when it is used by arr at podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c in line 61.

	Source	Destination
File	podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c	podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c
Line	68	69
Object	arr	arr

Code Snippet
File Name podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c
Method void PdfXRefStreamParserObject::ReadXRefTable()

```
....
68.      const PdfArray* arr;
69.      if (!arrObj.TryGetArray(arr) || arr->size() != 3)
```

Use of Uninitialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2216
Status	New

The variable declared in arr at podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c in line 61 is not initialized when it is used by arr at podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c in line 61.

	Source	Destination
File	podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c	podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c
Line	68	69
Object	arr	arr

Code Snippet
File Name podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c
Method void PdfXRefStreamParserObject::ReadXRefTable()

```
....
68.       const PdfArray* arr;
69.       if (!arrObj.TryGetArray(arr) || arr->size() != 3)
```

Use of Uninitialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2217
Status	New

The variable declared in arr at podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c in line 61 is not initialized when it is used by arr at podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c in line 61.

	Source	Destination
File	podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c	podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c
Line	68	77
Object	arr	arr

Code Snippet
File Name podofo@@podofo-0.10.0-rc1-CVE-2023-2241-TP.c
Method void PdfXRefStreamParserObject::ReadXRefTable()

```
....
68.      const PdfArray* arr;
....
77.          if (!(*arr)[i].TryGetNumber(num))
```

Short Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Short Overflow Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Short Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1116
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1136 of pymumu@@smartdns-Release41-RC1-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2023-31470-FP.c	pymumu@@smartdns-Release41-RC1-CVE-2023-31470-FP.c
Line	1145	1145
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_ipv4hint(struct dns_rr_nested *svcparam, unsigned char addr[][DNS_RR_A_LEN], int addr_num)

```
....
1145.       value = addr_num * DNS_RR_A_LEN;
```

Short Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1117
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1154 of pymumu@@smartdns-Release41-RC1-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2023-31470-FP.c	pymumu@@smartdns-Release41-RC1-CVE-2023-31470-FP.c
Line	1163	1163
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_ipv6hint(struct dns_rr_nested *svcparam, unsigned char addr[][DNS_RR_AAAA_LEN], int addr_num)

```
....
1163.       value = addr_num * DNS_RR_AAAA_LEN;
```

Short Overflow\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1118
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1165 of pymumu@@smartdns-Release43-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2023-31470-FP.c	pymumu@@smartdns-Release43-CVE-2023-31470-FP.c
Line	1174	1174
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_alpn(struct dns_rr_nested *svcparam, const char *alpn, int alpn_len)

```
....
1174.       value = alpn_len;
```

Short Overflow\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1119
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1197 of pymumu@@smartdns-Release43-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2023-31470-FP.c	pymumu@@smartdns-Release43-CVE-2023-31470-FP.c
Line	1206	1206
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_ipv4hint(struct dns_rr_nested *svcparam, unsigned char *addr[], int addr_num)

```
....
1206.       value = addr_num * DNS_RR_A_LEN;
```

Short Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1120
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1216 of pymumu@@smartdns-Release43-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2023-31470-FP.c	pymumu@@smartdns-Release43-CVE-2023-31470-FP.c
Line	1225	1225
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_ipv6hint(struct dns_rr_nested *svcparam, unsigned char *addr[], int addr_num)

```
....
1225.       value = addr_num * DNS_RR_AAAA_LEN;
```

Short Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1121
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1291 of pymumu@@smartdns-Release45-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release45-CVE-2023-31470-FP.c	pymumu@@smartdns-Release45-CVE-2023-31470-FP.c
Line	1300	1300
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release45-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_alpn(struct dns_rr_nested *svcparam, const char *alpn, int alpn_len)

```
....
1300.       value = alpn_len;
```

Short Overflow\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1122
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1323 of pymumu@@smartdns-Release45-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release45-CVE-2023-31470-FP.c	pymumu@@smartdns-Release45-CVE-2023-31470-FP.c
Line	1332	1332
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release45-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_ipv4hint(struct dns_rr_nested *svcparam, unsigned char *addr[], int addr_num)

```
....
1332.       value = addr_num * DNS_RR_A_LEN;
```

Short Overflow\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1123

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1342 of pymumu@@smartdns-Release45-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release45-CVE-2023-31470-FP.c	pymumu@@smartdns-Release45-CVE-2023-31470-FP.c
Line	1351	1351
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release45-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_ipv6hint(struct dns_rr_nested *svcparam, unsigned char *addr[], int addr_num)

```
....
1351.       value = addr_num * DNS_RR_AAAA_LEN;
```

Short Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1124
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1291 of pymumu@@smartdns-Release46-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release46-CVE-2023-31470-FP.c	pymumu@@smartdns-Release46-CVE-2023-31470-FP.c
Line	1300	1300
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release46-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_alpn(struct dns_rr_nested *svcparam, const char *alpn, int alpn_len)

```
....
1300.       value = alpn_len;
```

Short Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=1125
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1323 of pymumu@@smartdns-Release46-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release46-CVE-2023-31470-FP.c	pymumu@@smartdns-Release46-CVE-2023-31470-FP.c
Line	1332	1332
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release46-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_ipv4hint(struct dns_rr_nested *svcparam, unsigned char *addr[], int addr_num)

```
....
1332.       value = addr_num * DNS_RR_A_LEN;
```

Short Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1126
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1342 of pymumu@@smartdns-Release46-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release46-CVE-2023-31470-FP.c	pymumu@@smartdns-Release46-CVE-2023-31470-FP.c
Line	1351	1351
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release46-CVE-2023-31470-FP.c
Method int dns_HTTPS_add_ipv6hint(struct dns_rr_nested *svcparam, unsigned char *addr[], int addr_num)

```
....
1351.       value = addr_num * DNS_RR_AAAA_LEN;
```

Off by One Error in Methods

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Methods Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Off by One Error in Methods\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=435
Status	New

The buffer allocated by sizeof in pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 434 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	458	458
Object	buff	sizeof

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_vprintf(struct tlog_log *log, vprint_callback print_callback, void *userptr, const char *format, va_list ap)

```
....
458.          strncpy(buff, "[LOG TOO LONG, DISCARD]\n", sizeof(buff));
```

Off by One Error in Methods\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=436
Status	New

The buffer allocated by sizeof in pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 434 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	458	458
Object	buff	sizeof

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method	static int _tlog_vprintf(struct tlog_log *log, vprint_callback print_callback, void *userptr, const char *format, va_list ap)

```
....
458.          strncpy(buff, "[LOG TOO LONG, DISCARD]\n", sizeof(buff));
```

Off by One Error in Methods\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=437
Status	New

The buffer allocated by sizeof in pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 449 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	473	473
Object	buff	sizeof

Code Snippet	
File Name	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method	static int _tlog_vprintf(struct tlog_log *log, vprint_callback print_callback, void *userptr, const char *format, va_list ap)

```
....
473.          strncpy(buff, "[LOG TOO LONG, DISCARD]\n", sizeof(buff));
```

Off by One Error in Methods\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=438
Status	New

The buffer allocated by sizeof in pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 449 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	473	473
Object	buff	sizeof

Code Snippet

File Name	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method	static int _tlog_vprintf(struct tlog_log *log, vprint_callback print_callback, void *userptr, const char *format, va_list ap)

```
....
473.          strncpy(buff, "[LOG TOO LONG, DISCARD]\n", sizeof(buff));
```

Off by One Error in Methods\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=439
Status	New

The buffer allocated by sizeof in pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 483 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	507	507
Object	buff	sizeof

Code Snippet

File Name	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method	static int _tlog_vprintf(struct tlog_log *log, vprint_callback print_callback, void *userptr, const char *format, va_list ap)

```
....
507.          strncpy(buff, "[LOG TOO LONG, DISCARD]\n", sizeof(buff));
```

Off by One Error in Methods\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=440
Status	New

The buffer allocated by sizeof in pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 483 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	507	507
Object	buff	sizeof

Code Snippet	
File Name	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method	static int _tlog_vprintf(struct tlog_log *log, vprint_callback print_callback, void *userptr, const char *format, va_list ap)

```
....
507.          strncpy(buff, "[LOG TOO LONG, DISCARD]\n", sizeof(buff));
```

Off by One Error in Methods\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=441
Status	New

The buffer allocated by sizeof in pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 483 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	507	507
Object	buff	sizeof

Code Snippet	
File Name	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method	static int _tlog_vprintf(struct tlog_log *log, vprint_callback print_callback, void *userptr, const char *format, va_list ap)

```
....
507.          strncpy(buff, "[LOG TOO LONG, DISCARD]\n", sizeof(buff));
```

Off by One Error in Methods\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=442
Status	New

The buffer allocated by sizeof in pymumu@@smartdns-Release36-CVE-2024-24199-TP.c at line 483 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	507	507
Object	buff	sizeof

Code Snippet	
File Name	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method	static int _tlog_vprintf(struct tlog_log *log, vprint_callback print_callback, void *userptr, const char *format, va_list ap)

```
....
507.          strncpy(buff, "[LOG TOO LONG, DISCARD]\n", sizeof(buff));
```

Integer Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Integer Overflow Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Integer Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1110
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3542 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	3662	3662
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method	ldapServiceLookup(const char *purl, PQconninfoOption *options,

```
....
3662.              port = (int) lport;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1111
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 74 of postgres@@postgres-REL9_6_18-CVE-2022-2625-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2022-2625-TP.c	postgres@@postgres-REL9_6_18-CVE-2022-2625-TP.c
Line	104	104
Object	AssignExpr	AssignExpr

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2022-2625-TP.c
Method validOperatorName(const char *name)

```
....
104.                for (ic = len - 2; ic >= 0; ic--)
```

Integer Overflow\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1112
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3545 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	3665	3665
Object	AssignExpr	AssignExpr

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method ldapServiceLookup(const char *purl, PQconninfoOption *options,

```
....
3665.               port = (int) lport;
```

Integer Overflow\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1113
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 74 of postgres@@postgres-REL9_6_20-CVE-2022-2625-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2022-2625-TP.c	postgres@@postgres-REL9_6_20-CVE-2022-2625-TP.c
Line	104	104
Object	AssignExpr	AssignExpr

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2022-2625-TP.c
Method validOperatorName(const char *name)

```
....
104.                for (ic = len - 2; ic >= 0; ic--)
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1114
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 74 of postgres@@postgres-REL9_6_22-CVE-2022-2625-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	postgres@@postgres-REL9_6_22-CVE-2022-2625-TP.c	postgres@@postgres-REL9_6_22-CVE-2022-2625-TP.c
Line	104	104
Object	AssignExpr	AssignExpr

Code Snippet
File Name postgres@@postgres-REL9_6_22-CVE-2022-2625-TP.c
Method validOperatorName(const char *name)

```
....
104.                for (ic = len - 2; ic >= 0; ic--)
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1115
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 74 of postgres@@postgres-REL9_6_24-CVE-2022-2625-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	postgres@@postgres-REL9_6_24-CVE-2022-2625-TP.c	postgres@@postgres-REL9_6_24-CVE-2022-2625-TP.c
Line	104	104
Object	AssignExpr	AssignExpr

Code Snippet
File Name postgres@@postgres-REL9_6_24-CVE-2022-2625-TP.c
Method validOperatorName(const char *name)

```
....
104.              for (ic = len - 2; ic >= 0; ic--)
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Variable\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2218
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	210	879
Object	ReservedBackends	ReservedBackends

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method int ReservedBackends;

```
....
210.  int               ReservedBackends;
```

File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
879.        if (ReservedBackends >= MaxConnections)
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2219
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	208	898
Object	ReservedBackends	ReservedBackends

Code Snippet

File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c

Method int ReservedBackends;

```
....
208.  int               ReservedBackends;
```

File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c

Method PostmasterMain(int argc, char *argv[])

```
....
898.        if (ReservedBackends >= MaxConnections)
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2220
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-32027-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-32027-TP.c
Line	165	210
Object	lb0	lb0

Code Snippet

File Name	postgres@@postgres-REL9_6_18-CVE-2021-32027-TP.c
Method	array_prepend(PG_FUNCTION_ARGS)

```
....
165.        int                 lb0;
....
210.                eah->lbound[0] = lb0;
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2221
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-32027-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-32027-TP.c
Line	165	210
Object	lb0	lb0

Code Snippet

File Name	postgres@@postgres-REL9_6_20-CVE-2021-32027-TP.c
Method	array_prepend(PG_FUNCTION_ARGS)

```
....
165.        int                 lb0;
....
210.                eah->lbound[0] = lb0;
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2222
Status	New

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	475	528
Object	cmd_buflen	cmd_buflen

Code Snippet

File Name	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method	int pr_cmd_read(cmd_rec **res) {

```
....
475.    int cmd_buflen;
....
528.    if (cmd_buflen > cmd_bufsz) {
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2223
Status	New

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	480	533
Object	cmd_buflen	cmd_buflen

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method int pr_cmd_read(cmd_rec **res) {

```
....
480.    int cmd_buflen;
....
533.    if (cmd_buflen > cmd_bufsz) {
```

Heap Inspection

Query Path:
CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description
Heap Inspection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2043
Status	New

Method conninfo_uri_parse_options at line 4859 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	4920	4920
Object	password	password

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method conninfo_uri_parse_options(PQconninfoOption *options, const char *uri,

```
....
4920.                   const char *password = p + 1;
```

Heap Inspection\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2044
Status New

Method conninfo_uri_parse_options at line 4862 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	4923	4923
Object	password	password

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method conninfo_uri_parse_options(PQconninfoOption *options, const char *uri,

```
....
4923.                   const char *password = p + 1;
```

Heap Inspection\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2045
Status New

Method getPgPassFilename at line 5966 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c defines passfile_env, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passfile_env, this variable is never cleared from memory.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5968	5968
Object	passfile_env	passfile_env

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method getPgPassFilename(char *pgpassfile)

```
....
5968.       char     *passfile_env;
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2046
Status	New

Method getPgPassFilename at line 5985 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c defines passfile_env, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passfile_env, this variable is never cleared from memory.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5987	5987
Object	passfile_env	passfile_env

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method getPgPassFilename(char *pgpassfile)

```
....
5987.       char     *passfile_env;
```

Char Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Char Overflow Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1107
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 878 of pymumu@@smartdns-Release43-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2023-31470-FP.c	pymumu@@smartdns-Release43-CVE-2023-31470-FP.c
Line	887	887
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2023-31470-FP.c
Method int dns_add_TXT(struct dns_packet *packet, dns_rr_type type, const char *domain, int ttl, const char *text)

```
....
887.        data[0] = rr_len;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1108
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 939 of pymumu@@smartdns-Release45-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release45-CVE-2023-31470-FP.c	pymumu@@smartdns-Release45-CVE-2023-31470-FP.c
Line	948	948
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release45-CVE-2023-31470-FP.c
Method int dns_add_TXT(struct dns_packet *packet, dns_rr_type type, const char *domain, int ttl, const char *text)

```
....
948.        data[0] = rr_len;
```

Char Overflow\Path 3:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1109
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 939 of pymumu@@smartdns-Release46-CVE-2023-31470-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	pymumu@@smartdns-Release46-CVE-2023-31470-FP.c	pymumu@@smartdns-Release46-CVE-2023-31470-FP.c
Line	948	948
Object	AssignExpr	AssignExpr

Code Snippet
File Name pymumu@@smartdns-Release46-CVE-2023-31470-FP.c
Method int dns_add_TXT(struct dns_packet *packet, dns_rr_type type, const char *domain, int ttl, const char *text)

```
....
948.        data[0] = rr_len;
```

Stored Buffer Overflow fgets

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow fgets Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description
Stored Buffer Overflow fgets\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2392
Status	New

The size of the buffer used by PasswordFromFile in BinaryExpr, at line 5842 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that PasswordFromFile passes to BinaryExpr, at line 5842 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c, to overwrite the target buffer.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5916	5916
Object	BinaryExpr	BinaryExpr

Code Snippet	
File Name	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method	PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5916.             if (fgets(buf.data + buf.len, buf.maxlen - buf.len,
fp) == NULL)
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=485
Status	New

The variable declared in null at pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c in line 1232 is not initialized when it is used by mutex_frm at pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c in line 1232.

	Source	Destination
File	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Line	1236	1274
Object	null	mutex_frm

Code Snippet	
File Name	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Method	int task_get_references(davs2_t *h, int64_t pts, int64_t dts)

```
....
1236.      davs2_frame_t  *frame = NULL;
....
1274.              davs2_thread_mutex_unlock(&frame->mutex_frm);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=486
Status	New

The variable declared in null at pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c in line 1232 is not initialized when it is used by mutex_frm at pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c in line 1232.

	Source	Destination
File	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c	pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Line	1236	1265
Object	null	mutex_frm

Code Snippet
File Name pkuvcl@@davs2-1.7-CVE-2022-36647-TP.c
Method int task_get_references(davs2_t *h, int64_t pts, int64_t dts)

```
....
1236.       davs2_frame_t  *frame = NULL;
....
1265.               davs2_thread_mutex_lock(&frame->mutex_frm);
```

NULL Pointer Dereference\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=487
Status New

The variable declared in null at postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c in line 167 is not initialized when it is used by classId at postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c in line 2985.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	191	3062
Object	null	classId

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method get_extension_name(Oid ext_oid)

```
....
191.                result = NULL;
```

File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method ExecAlterExtensionContentsStmt(AlterExtensionContentsStmt *stmt,

```
....
3062.               recordExtObjInitPriv(object.objectId, object.classId);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=488
Status	New

The variable declared in null at postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c in line 167 is not initialized when it is used by objectId at postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c in line 2985.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	191	3062
Object	null	objectId

Code Snippet

File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c

Method get_extension_name(Oid ext_oid)

```
....
191.              result = NULL;
```

File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c

Method ExecAlterExtensionContentsStmt(AlterExtensionContentsStmt *stmt,

```
....
3062.             recordExtObjInitPriv(object.objectId, object.classId);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=489
Status	New

The variable declared in null at postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c in line 3528 is not initialized when it is used by tg_newtuple at postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c in line 3528.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	3605	3602

Object	null	tg_newtuple

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method AfterTriggerExecute(AfterTriggerEvent event,

```
....
3605.                           ExecMaterializeSlot(trig_tuple_slot2) :
NULL;
....
3602.                    LocTriggerData.tg_newtuple =
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=490
Status	New

The variable declared in null at postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c in line 4074 is not initialized when it is used by head at postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c in line 3320.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	4098	3388
Object	null	head

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method AfterTriggerFireDeferred(void)

```
....
4098.       while (afterTriggerMarkEvents(events, NULL, false))
```

File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method afterTriggerAddEvent(AfterTriggerEventList *events,

```
....
3388.             if (events->head == NULL)
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=491
Status	New

The variable declared in null at postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c in line 4494 is not initialized when it is used by head at postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c in line 3320.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	4738	3388
Object	null	head

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method AfterTriggerSetState(ConstraintsSetStmt *stmt)

```
....
4738.             while (afterTriggerMarkEvents(events, NULL, true))
```

File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method afterTriggerAddEvent(AfterTriggerEventList *events,

```
....
3388.             if (events->head == NULL)
```

NULL Pointer Dereference\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=492
Status New

The variable declared in null at postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c in line 6028 is not initialized when it is used by pw_dir at postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c in line 6028.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	6033	6038
Object	null	pw_dir

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method pqGetHomeDirectory(char *buf, int bufsize)

```
....
6033.       struct passwd *pwd = NULL;
....
6038.       strlcpy(buf, pwd->pw_dir, bufsize);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=493
Status	New

The variable declared in null at postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c in line 6047 is not initialized when it is used by pw_dir at postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c in line 6047.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	6052	6057
Object	null	pw_dir

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method pqGetHomeDirectory(char *buf, int bufsize)

```
....
6052.       struct passwd *pwd = NULL;
....
6057.       strlcpy(buf, pwd->pw_dir, bufsize);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=494
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 892 is not initialized when it is used by argv at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 616.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	896	770
Object	null	argv

Code Snippet

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
896.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method int pr_cmd_dispatch_phase(cmd_rec *cmd, int phase, int flags) {

```
....
770.             (char *) cmd->argv[0]);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=495
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 892 is not initialized when it is used by argv at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 616.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	896	775
Object	null	argv

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
896.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method int pr_cmd_dispatch_phase(cmd_rec *cmd, int phase, int flags) {

```
....
775.             (char *) cmd->argv[0]);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=496
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 892 is not initialized when it is used by argv at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 231.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	896	430
Object	null	argv

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
896.      cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static int _dispatch(cmd_rec *cmd, int cmd_type, int validate, char *match) {

```
....
430.      if (strchr(cmd->argv[0], '_') == NULL) {
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=497
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 892 is not initialized when it is used by tmp_pool at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 231.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	896	288
Object	null	tmp_pool

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
896.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c

Method static int _dispatch(cmd_rec *cmd, int cmd_type, int validate, char *match) {

```
....
288.         if (cmd->tmp_pool == NULL) {
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=498
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 892 is not initialized when it is used by notes at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 593.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	896	597
Object	null	notes

Code Snippet

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c

Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
896.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c

Method static int set_cmd_start_ms(cmd_rec *cmd) {

```
....
597.     if (cmd->notes == NULL) {
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=499
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 892 is not initialized when it is used by cmd_class at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 616.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	896	658
Object	null	cmd_class

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
896.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method int pr_cmd_dispatch_phase(cmd_rec *cmd, int phase, int flags) {

```
....
658.    if (cmd->cmd_class == 0) {
```

NULL Pointer Dereference\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=500
Status New

The variable declared in null at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 892 is not initialized when it is used by cmd_id at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 616.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	896	662
Object	null	cmd_id

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
896.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c

Method int pr_cmd_dispatch_phase(cmd_rec *cmd, int phase, int flags) {

```
....
662.    if (cmd->cmd_id == 0) {
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=501
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 892 is not initialized when it is used by pool at proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c in line 616.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	896	652
Object	null	pool

Code Snippet

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c

Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
896.      cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c

Method int pr_cmd_dispatch_phase(cmd_rec *cmd, int phase, int flags) {

```
....
652.    pr_response_set_pool(cmd->pool);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=502
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 902 is not initialized when it is used by argv at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 621.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	906	780
Object	null	argv

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
906.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method int pr_cmd_dispatch_phase(cmd_rec *cmd, int phase, int flags) {

```
....
780.             (char *) cmd->argv[0]);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=503
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 902 is not initialized when it is used by argv at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 621.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	906	785
Object	null	argv

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
906.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method int pr_cmd_dispatch_phase(cmd_rec *cmd, int phase, int flags) {

```
....
785.            (char *) cmd->argv[0]);
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=504
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 902 is not initialized when it is used by argv at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 232.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	906	434
Object	null	argv

Code Snippet

File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c

Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
906.      cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c

Method static int _dispatch(cmd_rec *cmd, int cmd_type, int validate, char *match) {

```
....
434.      if (strchr(cmd->argv[0], '_') == NULL) {
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=505
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 902 is not initialized when it is used by tmp_pool at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 232.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c

Line	906	289
Object	null	tmp_pool

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
906.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static int _dispatch(cmd_rec *cmd, int cmd_type, int validate, char *match) {

```
....
289.         if (cmd->tmp_pool == NULL) {
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=506
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 902 is not initialized when it is used by notes at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 598.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	906	602
Object	null	notes

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
906.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static int set_cmd_start_ms(cmd_rec *cmd) {

```
....
602.     if (cmd->notes == NULL) {
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=507
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 902 is not initialized when it is used by cmd_class at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 621.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	906	663
Object	null	cmd_class

Code Snippet

File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c

Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
906.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c

Method int pr_cmd_dispatch_phase(cmd_rec *cmd, int phase, int flags) {

```
....
663.     if (cmd->cmd_class == 0) {
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=508
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 902 is not initialized when it is used by cmd_id at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 621.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	906	667
Object	null	cmd_id

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
906.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c

Method int pr_cmd_dispatch_phase(cmd_rec *cmd, int phase, int flags) {

```
....
667.     if (cmd->cmd_id == 0) {
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=509
Status	New

The variable declared in null at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 902 is not initialized when it is used by pool at proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c in line 621.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	906	657
Object	null	pool

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void cmd_loop(server_rec *server, conn_t *c) {

```
....
906.       cmd_rec *cmd = NULL;
```

File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c

Method int pr_cmd_dispatch_phase(cmd_rec *cmd, int phase, int flags) {

```
....
657.     pr_response_set_pool(cmd->pool);
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=510
Status	New

The variable declared in null at projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c in line 390 is not initialized when it is used by vm at projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c in line 390.

	Source	Destination
File	projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c	projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c
Line	410	439
Object	null	vm

Code Snippet
File Name projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c
Method static struct ptirq_remapping_info *add_intx_remapping(struct acrn_vm *vm, uint32_t virt_gsi,

```
....
410.                                    entry = NULL;
....
439.                        entry->vm->vm_id, virt_gsi, phys_gsi);
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=511
Status	New

The variable declared in null at projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c in line 390 is not initialized when it is used by vm at projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c in line 390.

	Source	Destination
File	projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c	projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c
Line	424	439
Object	null	vm

Code Snippet
File Name projectacrn@@acrn-hypervisor-v1.6.1-CVE-2021-36148-TP.c
Method static struct ptirq_remapping_info *add_intx_remapping(struct acrn_vm *vm, uint32_t virt_gsi,

```
....
424.                    entry = NULL;
....
439.                    entry->vm->vm_id, virt_gsi, phys_gsi);
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=512
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1248.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1368	1259
Object	null	log

Code Snippet

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method static void _tlog_write_one_segment_log(struct tlog_log *log, char *buff, int bufflen)

```
....
1259.           log->output_func(log, segment_head->data, segment_head->len - 1);
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=513
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1283.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1368	1296
Object	null	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method static void _tlog_work_write(struct tlog_log *log, int log_len, int log_extlen, int log_dropped)

```
....
1296.          log->output_func(log, dropmsg, strnlen(dropmsg,
sizeof(dropmsg)));
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=514
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1274.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1368	1279
Object	null	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method	static void _tlog_write_buff_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1279.          log->output_func(log, log->buff, log_extlen);
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=515
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1274.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1368	1276
Object	null	log

Code Snippet

File Name	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method	static void *_tlog_work(void *arg)

```
....
1368.                      log = NULL;
```

File Name	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method	static void _tlog_write_buff_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1276.      log->output_func(log, log->buff + log->start, log_len);
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=516
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by buff at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1265.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-	pymumu@@smartdns-Release31-CVE-

	2024-24198-TP.c	2024-24198-TP.c
Line	1368	1267
Object	null	buff

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method static void _tlog_write_segments_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1267.       _tlog_write_one_segment_log(log, log->buff + log->start,
log_len);
```

NULL Pointer Dereference\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=517
Status New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by buff at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1274.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1368	1276
Object	null	buff

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method static void _tlog_write_buff_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1276.       log->output_func(log, log->buff + log->start, log_len);
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=518
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by lock at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1237.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1368	1244
Object	null	lock

Code Snippet

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method static void _tlog_wakeup_waiters(struct tlog_log *log)

```
....
1244.       pthread_mutex_unlock(&log->lock);
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=519
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by lock at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1237.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Line	1368	1239
Object	null	lock

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void _tlog_wakeup_waiters(struct tlog_log *log)

```
....
1239.       pthread_mutex_lock(&log->lock);
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=520
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by segment_log at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1283.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1368	1286
Object	null	segment_log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void _tlog_work_write(struct tlog_log *log, int log_len, int log_extlen, int log_dropped)

```
....
1286.       if (log->segment_log) {
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=521
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by start at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1265.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1368	1267
Object	null	start

Code Snippet

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method static void _tlog_write_segments_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1267.       _tlog_write_one_segment_log(log, log->buff + log->start,
log_len);
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=522
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1320 is not initialized when it is used by start at pymumu@@smartdns-Release31-CVE-2024-24198-TP.c in line 1274.

	Source	Destination

File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1368	1276
Object	null	start

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static void _tlog_write_buff_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1276.      log->output_func(log, log->buff + log->start, log_len);
```

NULL Pointer Dereference\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=523
Status New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1248.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1259
Object	null	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void _tlog_write_one_segment_log(struct tlog_log *log, char *buff, int bufflen)

```
....
1259.          log->output_func(log, segment_head->data, segment_head-
>len - 1);
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=524
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1283.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1296
Object	null	log

Code Snippet

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method static void _tlog_work_write(struct tlog_log *log, int log_len, int log_extlen, int log_dropped)

```
....
1296.          log->output_func(log, dropmsg, strnlen(dropmsg,
sizeof(dropmsg)));
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=525
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1274.

	Source	Destination

File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1279
Object	null	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void _tlog_write_buff_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1279.          log->output_func(log, log->buff, log_extlen);
```

NULL Pointer Dereference\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=526
Status New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1274.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1276
Object	null	log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void _tlog_write_buff_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1276.       log->output_func(log, log->buff + log->start, log_len);
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=527
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by buff at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1265.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1267
Object	null	buff

Code Snippet

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method static void _tlog_write_segments_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1267.       _tlog_write_one_segment_log(log, log->buff + log->start,
log_len);
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=528
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by buff at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1274.

	Source	Destination

File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1276
Object	null	buff

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void _tlog_write_buff_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1276.      log->output_func(log, log->buff + log->start, log_len);
```

NULL Pointer Dereference\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=529
Status New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by lock at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1237.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1244
Object	null	lock

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void _tlog_wakeup_waiters(struct tlog_log *log)

```
....
1244.       pthread_mutex_unlock(&log->lock);
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=530
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by lock at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1237.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1239
Object	null	lock

Code Snippet

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method static void _tlog_wakeup_waiters(struct tlog_log *log)

```
....
1239.       pthread_mutex_lock(&log->lock);
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=531
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by segment_log at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1283.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-	pymumu@@smartdns-Release31-CVE-

	2024-24199-TP.c	2024-24199-TP.c
Line	1368	1286
Object	null	segment_log

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method static void _tlog_work_write(struct tlog_log *log, int log_len, int log_extlen, int log_dropped)

```
....
1286.       if (log->segment_log) {
```

NULL Pointer Dereference\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=532
Status New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by start at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1265.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1267
Object	null	start

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method static void _tlog_write_segments_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1267.       _tlog_write_one_segment_log(log, log->buff + log->start,
log_len);
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=533
Status	New

The variable declared in null at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1320 is not initialized when it is used by start at pymumu@@smartdns-Release31-CVE-2024-24199-TP.c in line 1274.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1368	1276
Object	null	start

Code Snippet

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method static void *_tlog_work(void *arg)

```
....
1368.                       log = NULL;
```

File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method static void _tlog_write_buff_log(struct tlog_log *log, int log_len, int log_extlen)

```
....
1276.       log->output_func(log, log->buff + log->start, log_len);
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=534
Status	New

The variable declared in null at pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c in line 1339 is not initialized when it is used by log at pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c in line 1267.

	Source	Destination

File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1390	1278
Object	null	log

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static void *_tlog_work(void *arg)

```
....
1390.                       log = NULL;
```

File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static void _tlog_write_one_segment_log(struct tlog_log *log, char *buff, int bufflen)

```
....
1278.          log->output_func(log, segment_head->data, segment_head->len - 1);
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

NIST SP 800-53: SI-11 Error Handling (P2)

Description
Unchecked Return Value\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2886
Status	New

The pkgconf_tuple_parse method calls the strdup function, at line 251 of pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Line	336	336
Object	strdup	strdup

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c

Method	pkgconf_tuple_parse(const pkgconf_client_t *client, pkgconf_list_t *vars, const char *value)

```
....
336.                return strdup(cleanpath);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2887
Status	New

The pkgconf_tuple_parse method calls the strdup function, at line 251 of pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Line	339	339
Object	strdup	strdup

Code Snippet	
File Name	pkgconf@@pkgconf-pkgconf-1.7.0-CVE-2023-24056-TP.c
Method	pkgconf_tuple_parse(const pkgconf_client_t *client, pkgconf_list_t *vars, const char *value)

```
....
339.        return strdup(buf);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2888
Status	New

The pkgconf_tuple_parse method calls the strdup function, at line 251 of pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Line	348	348
Object	strdup	strdup

Code Snippet	
File Name	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Method	pkgconf_tuple_parse(const pkgconf_client_t *client, pkgconf_list_t *vars, const char *value)

```
....
348.                return strdup(cleanpath);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2889
Status	New

The pkgconf_tuple_parse method calls the strdup function, at line 251 of pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Line	351	351
Object	strdup	strdup

Code Snippet	
File Name	pkgconf@@pkgconf-pkgconf-1.7.4-CVE-2023-24056-FP.c
Method	pkgconf_tuple_parse(const pkgconf_client_t *client, pkgconf_list_t *vars, const char *value)

```
....
351.        return strdup(buf);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2890
Status	New

The pkgconf_tuple_parse method calls the strdup function, at line 251 of pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c

Line	348	348
Object	strdup	strdup

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_parse(const pkgconf_client_t *client, pkgconf_list_t *vars, const char *value)

```
....
348.              return strdup(cleanpath);
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2891
Status New

The pkgconf_tuple_parse method calls the strdup function, at line 251 of pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Line	351	351
Object	strdup	strdup

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.8.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_parse(const pkgconf_client_t *client, pkgconf_list_t *vars, const char *value)

```
....
351.          return strdup(buf);
```

Unchecked Return Value\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2892
Status New

The pkgconf_tuple_parse method calls the strdup function, at line 287 of pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Line	386	386
Object	strdup	strdup

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_parse(const pkgconf_client_t *client, pkgconf_list_t *vars, const char *value, unsigned int flags)

```
....
386.                return strdup(cleanpath);
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2893
Status New

The pkgconf_tuple_parse method calls the strdup function, at line 287 of pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c	pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Line	389	389
Object	strdup	strdup

Code Snippet
File Name pkgconf@@pkgconf-pkgconf-1.9.0-CVE-2023-24056-FP.c
Method pkgconf_tuple_parse(const pkgconf_client_t *client, pkgconf_list_t *vars, const char *value, unsigned int flags)

```
....
389.        return strdup(buf);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2894
Status New

The get_extension_control_directory method calls the snprintf function, at line 353 of postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	360	360
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method get_extension_control_directory(void)

```
....
360.        snprintf(result, MAXPGPATH, "%s/extension", sharepath);
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2895
Status New

The get_extension_control_filename method calls the snprintf function, at line 366 of postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	373	373
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method get_extension_control_filename(const char *extname)

```
....
373.        snprintf(result, MAXPGPATH, "%s/extension/%s.control",
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2896
Status New

The get_extension_script_directory method calls the snprintf function, at line 380 of postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	397	397
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method get_extension_script_directory(ExtensionControlFile *control)

```
....
397.        snprintf(result, MAXPGPATH, "%s/%s", sharepath, control->directory);
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2897
Status New

The get_extension_aux_control_filename method calls the snprintf function, at line 403 of postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	412	412
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method get_extension_aux_control_filename(ExtensionControlFile *control,

```
....
412.        snprintf(result, MAXPGPATH, "%s/%s--%s.control",
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=2898
Status	New

The get_extension_script_filename method calls the snprintf function, at line 421 of postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	431	431
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method get_extension_script_filename(ExtensionControlFile *control,

```
....
431.                snprintf(result, MAXPGPATH, "%s/%s--%s--%s.sql",
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2899
Status	New

The get_extension_script_filename method calls the snprintf function, at line 421 of postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	434	434
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method get_extension_script_filename(ExtensionControlFile *control,

```
....
434.                snprintf(result, MAXPGPATH, "%s/%s--%s.sql",
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2900
Status	New

The CreateTrigger method calls the snprintf function, at line 138 of postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	518	518
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method CreateTrigger(CreateTrigStmt *stmt, const char *queryString,

```
....
518.                snprintf(internaltrigname, sizeof(internaltrigname),
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2901
Status	New

The PrintQueryStatus method calls the snprintf function, at line 1084 of postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	1103	1103
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1103.        snprintf(buf, sizeof(buf), "%u", (unsigned int)
PQoidValue(results));
```

Unchecked Return Value\Path 17:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2902
Status	New

The ExecQueryUsingCursor method calls the snprintf function, at line 1454 of postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	1522	1522
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method ExecQueryUsingCursor(const char *query, double *elapsed_msec)

```
....
1522.       snprintf(fetch_cmd, sizeof(fetch_cmd),
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2903
Status	New

The PostmasterMain method calls the snprintf function, at line 566 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	746	746
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
746.                            snprintf(ExtraOptions +
strlen(ExtraOptions),
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2904
Status	New

The checkDataDir method calls the snprintf function, at line 1444 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	1516	1516
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method checkDataDir(void)

```
....
1516.        snprintf(path, sizeof(path), "%s/global/pg_control",
DataDir);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2905
Status	New

The CleanupBackgroundWorker method calls the snprintf function, at line 3098 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	3119	3119
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method CleanupBackgroundWorker(int pid,

```
....
3119.             snprintf(namebuf, MAXPGPATH, "%s: %s", _("worker
process"),
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2906
Status	New

The report_fork_failure_to_client method calls the snprintf function, at line 4068 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4074	4074
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method report_fork_failure_to_client(Port *port, int errnum)

```
....
4074.       snprintf(buffer, sizeof(buffer), "E%s%s\n",
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2907
Status	New

The BackendInitialize method calls the snprintf function, at line 4101 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4173	4173
Object	snprintf	snprintf

Code Snippet

File Name	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method	BackendInitialize(Port *port)

```
....
4173.              snprintf(remote_ps_data, sizeof(remote_ps_data), "%s",
remote_host);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2908
Status	New

The BackendInitialize method calls the snprintf function, at line 4101 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4175	4175
Object	snprintf	snprintf

Code Snippet

File Name	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method	BackendInitialize(Port *port)

```
....
4175.              snprintf(remote_ps_data, sizeof(remote_ps_data),
"%s(%s)", remote_host, remote_port);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2909
Status	New

The internal_forkexec method calls the snprintf function, at line 4407 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4419	4419

Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method internal_forkexec(int argc, char *argv[], Port *port)

```
....
4419.       snprintf(tmpfilename, MAXPGPATH, "%s/%s.backend_var.%d.%lu",
```

Unchecked Return Value\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2910
Status New

The StartChildProcess method calls the snprintf function, at line 5272 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5289	5289
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method StartChildProcess(AuxProcType type)

```
....
5289.       snprintf(typebuf, sizeof(typebuf), "-x%d", type);
```

Unchecked Return Value\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2911
Status New

The bgworker_forkexec method calls the snprintf function, at line 5588 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c

Line	5594	5594
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method bgworker_forkexec(int shmem_slot)

```
....
5594.       snprintf(forkav, MAXPGPATH, "--forkbgworker=%d",
shmem_slot);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2912
Status	New

The connectDBStart method calls the snprintf function, at line 1495 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	1538	1538
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method connectDBStart(PGconn *conn)

```
....
1538.       snprintf(portstr, sizeof(portstr), "%d", portnum);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2913
Status	New

The parseServiceInfo method calls the snprintf function, at line 3998 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	4031	4031
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method parseServiceInfo(PQconninfoOption *options, PQExpBuffer errorMessage)

```
....
4031.             snprintf(serviceFile, MAXPGPATH, "%s/%s", homedir,
".pg_service.conf");
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2914
Status	New

The parseServiceInfo method calls the snprintf function, at line 3998 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	4046	4046
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method parseServiceInfo(PQconninfoOption *options, PQExpBuffer errorMessage)

```
....
4046.       snprintf(serviceFile, MAXPGPATH, "%s/pg_service.conf",
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2915
Status	New

The PQsetClientEncoding method calls the sprintf function, at line 5644 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5666	5666
Object	sprintf	sprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQsetClientEncoding(PGconn *conn, const char *encoding)

```
....
5666.       sprintf(qbuf, query, encoding);
```

Unchecked Return Value\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2916
Status New

The getPgPassFilename method calls the snprintf function, at line 5966 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5979	5979
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method getPgPassFilename(char *pgpassfile)

```
....
5979.             snprintf(pgpassfile, MAXPGPATH, "%s/%s", homedir,
PGPASSFILE);
```

Unchecked Return Value\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2917
Status New

The PostmasterMain method calls the snprintf function, at line 578 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	765	765
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
765.                            snprintf(ExtraOptions +
strlen(ExtraOptions),
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2918
Status	New

The checkDataDir method calls the snprintf function, at line 1463 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	1535	1535
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method checkDataDir(void)

```
....
1535.       snprintf(path, sizeof(path), "%s/global/pg_control",
DataDir);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=2919
Status	New

The CleanupBackgroundWorker method calls the snprintf function, at line 3110 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	3131	3131
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method CleanupBackgroundWorker(int pid,

```
....
3131.              snprintf(namebuf, MAXPGPATH, "%s: %s", _("worker
process"),
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2920
Status	New

The report_fork_failure_to_client method calls the snprintf function, at line 4096 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	4102	4102
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method report_fork_failure_to_client(Port *port, int errnum)

```
....
4102.       snprintf(buffer, sizeof(buffer), "E%s%s\n",
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2921
Status	New

The BackendInitialize method calls the snprintf function, at line 4129 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	4209	4209
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method BackendInitialize(Port *port)

```
....
4209.             snprintf(remote_ps_data, sizeof(remote_ps_data), "%s",
remote_host);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2922
Status	New

The BackendInitialize method calls the snprintf function, at line 4129 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	4211	4211
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method BackendInitialize(Port *port)

```
....
4211.             snprintf(remote_ps_data, sizeof(remote_ps_data),
"%s(%s)", remote_host, remote_port);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2923
Status	New

The internal_forkexec method calls the snprintf function, at line 4443 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	4455	4455
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method internal_forkexec(int argc, char *argv[], Port *port)

```
....
4455.       snprintf(tmpfilename, MAXPGPATH, "%s/%s.backend_var.%d.%lu",
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2924
Status	New

The StartChildProcess method calls the snprintf function, at line 5351 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5368	5368
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method StartChildProcess(AuxProcType type)

```
....
5368.       snprintf(typebuf, sizeof(typebuf), "-x%d", type);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2925
Status	New

The bgworker_forkexec method calls the snprintf function, at line 5667 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5673	5673
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method bgworker_forkexec(int shmem_slot)

```
....
5673.       snprintf(forkav, MAXPGPATH, "--forkbgworker=%d",
shmem_slot);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2926
Status	New

The connectDBStart method calls the snprintf function, at line 1495 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	1538	1538
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method connectDBStart(PGconn *conn)

```
....
1538.       snprintf(portstr, sizeof(portstr), "%d", portnum);
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2927
Status	New

The parseServiceInfo method calls the snprintf function, at line 4001 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	4034	4034
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method parseServiceInfo(PQconninfoOption *options, PQExpBuffer errorMessage)

```
....
4034.             snprintf(serviceFile, MAXPGPATH, "%s/%s", homedir,
".pg_service.conf");
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2928
Status	New

The parseServiceInfo method calls the snprintf function, at line 4001 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	4049	4049
Object	snprintf	snprintf

Code Snippet

File Name	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method	parseServiceInfo(PQconninfoOption *options, PQExpBuffer errorMessage)

```
....
4049.       snprintf(serviceFile, MAXPGPATH, "%s/pg_service.conf",
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2929
Status	New

The PQsetClientEncoding method calls the sprintf function, at line 5647 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5669	5669
Object	sprintf	sprintf

Code Snippet

File Name	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method	PQsetClientEncoding(PGconn *conn, const char *encoding)

```
....
5669.       sprintf(qbuf, query, encoding);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2930
Status	New

The getPgPassFilename method calls the snprintf function, at line 5985 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5998	5998
Object	snprintf	snprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method getPgPassFilename(char *pgpassfile)

```
....
5998.             snprintf(pgpassfile, MAXPGPATH, "%s/%s", homedir,
PGPASSFILE);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2931
Status	New

The system_alloc method calls the malloc function, at line 149 of protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Line	151	151
Object	malloc	malloc

Code Snippet
File Name protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
151.         return malloc(size);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2932
Status	New

The system_alloc method calls the malloc function, at line 151 of protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Line	154	154

Object	malloc	malloc

Code Snippet
File Name protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Method system_alloc(void *allocator_data, size_t size)

```
....
154.        return malloc(size);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2933
Status	New

The Navigator::check_traffic method calls the snprintf function, at line 1008 of PX4@@PX4-Autopilot-v1.11.0-rc1-CVE-2024-30800-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	PX4@@PX4-Autopilot-v1.11.0-rc1-CVE-2024-30800-TP.c	PX4@@PX4-Autopilot-v1.11.0-rc1-CVE-2024-30800-TP.c
Line	1046	1046
Object	snprintf	snprintf

Code Snippet
File Name PX4@@PX4-Autopilot-v1.11.0-rc1-CVE-2024-30800-TP.c
Method void Navigator::check_traffic()

```
....
1046.                    snprintf(&uas_id[i * 2], sizeof(uas_id) - i * 2,
"%02x", tr.uas_id[PX4_GUID_BYTE_LENGTH - 5 + i]);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2934
Status	New

The Navigator::check_traffic method calls the snprintf function, at line 1013 of PX4@@PX4-Autopilot-v1.11.2-CVE-2024-30800-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	PX4@@PX4-Autopilot-v1.11.2-CVE-2024-30800-TP.c	PX4@@PX4-Autopilot-v1.11.2-CVE-2024-30800-TP.c

Line	1051	1051
Object	snprintf	snprintf

Code Snippet
File Name PX4@@PX4-Autopilot-v1.11.2-CVE-2024-30800-TP.c
Method void Navigator::check_traffic()

```
....
1051.                   snprintf(&uas_id[i * 2], sizeof(uas_id) - i * 2,
"%02x", tr.uas_id[PX4_GUID_BYTE_LENGTH - 5 + i]);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2935
Status	New

The Navigator::check_traffic method calls the snprintf function, at line 1091 of PX4@@PX4-Autopilot-v1.12.0-beta1-CVE-2024-30800-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	PX4@@PX4-Autopilot-v1.12.0-beta1-CVE-2024-30800-TP.c	PX4@@PX4-Autopilot-v1.12.0-beta1-CVE-2024-30800-TP.c
Line	1129	1129
Object	snprintf	snprintf

Code Snippet
File Name PX4@@PX4-Autopilot-v1.12.0-beta1-CVE-2024-30800-TP.c
Method void Navigator::check_traffic()

```
....
1129.                   snprintf(&uas_id[i * 2], sizeof(uas_id) - i * 2,
"%02x", tr.uas_id[PX4_GUID_BYTE_LENGTH - 5 + i]);
```

Improper Resource Access Authorization

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2393
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	1217	1217
Object	fgets	fgets

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1217.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2394
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	4087	4087
Object	fgets	fgets

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method parseServiceFile(const char *serviceFile,

```
....
4087.       while ((line = fgets(buf, sizeof(buf), f)) != NULL)
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2395
Status	New

	Source	Destination

File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5913	5913
Object	fgets	fgets

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5913.             if (fgets(buf, sizeof(buf), fp) == NULL)
```

Improper Resource Access Authorization\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2396
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	4090	4090
Object	fgets	fgets

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method parseServiceFile(const char *serviceFile,

```
....
4090.       while ((line = fgets(buf, sizeof(buf), f)) != NULL)
```

Improper Resource Access Authorization\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2397
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5916	5916
Object	fgets	fgets

Code Snippet	
File Name	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method	PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5916.             if (fgets(buf.data + buf.len, buf.maxlen - buf.len,
fp) == NULL)
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2398
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	1217	1217
Object	buf	buf

Code Snippet	
File Name	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method	SendQuery(const char *query)

```
....
1217.             if (fgets(buf, sizeof(buf), stdin) != NULL)
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2399
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	4087	4087
Object	buf	buf

Code Snippet	
File Name	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method	parseServiceFile(const char *serviceFile,

```
....
4087.       while ((line = fgets(buf, sizeof(buf), f)) != NULL)
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2400
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5913	5913
Object	buf	buf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5913.             if (fgets(buf, sizeof(buf), fp) == NULL)
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2401
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	4090	4090
Object	buf	buf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method parseServiceFile(const char *serviceFile,

```
....
4090.       while ((line = fgets(buf, sizeof(buf), f)) != NULL)
```

Improper Resource Access Authorization\Path 10:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2402
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5916	5916
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5916.             if (fgets(buf.data + buf.len, buf.maxlen - buf.len,
fp) == NULL)
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2403
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Line	3149	3149
Object	buf	buf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-14350-TP.c
Method read_whole_file(const char *filename, int *length)

```
....
3149.       *length = fread(buf, 1, bytes_to_read, file);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2404
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	6161	6161
Object	Address	Address

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method read_backend_variables(char *id, Port *port)

```
....
6161.       if (fread(&param, sizeof(param), 1, fp) != 1)
```

Improper Resource Access Authorization\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2405
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	6239	6239
Object	Address	Address

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method read_backend_variables(char *id, Port *port)

```
....
6239.       if (fread(&param, sizeof(param), 1, fp) != 1)
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2406
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	579	579

Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method PSQLexec(const char *query)

```
....
579.                    fprintf(pset.logfile,
```

Improper Resource Access Authorization\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2407
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	669	669
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method PSQLexecWatch(const char *query, const printQueryOpt *opt)

```
....
669.                    fprintf(pset.queryFout, "%s\n%s\n\n", opt-
>title, PQcmdStatus(res));
```

Improper Resource Access Authorization\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2408
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	715	715
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method PrintNotifications(void)

```
....
715.                    fprintf(pset.queryFout, _("Asynchronous
notification \"%s\" with payload \"%s\" received from server process
with PID %d.\n"),
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2409
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	718	718
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method PrintNotifications(void)

```
....
718.                    fprintf(pset.queryFout, _("Asynchronous
notification \"%s\" received from server process with PID %d.\n"),
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2410
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	1097	1097
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1097.                    fprintf(pset.queryFout, "%s\n",
PQcmdStatus(results));
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2411
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	1101	1101
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method PrintQueryStatus(PGresult *results)

```
....
1101.             fprintf(pset.logfile, "%s\n", PQcmdStatus(results));
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2412
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	1231	1231
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method SendQuery(const char *query)

```
....
1231.             fprintf(pset.logfile,
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2413
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	1196	1196
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
1196.                   fprintf(fpidfile, "%d\n", MyProcPid);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2414
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5492	5492
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method CreateOptsFile(int argc, char *argv[], char *fullprogname)

```
....
5492.       fprintf(fp, "%s", fullprogname);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2415
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5494	5494
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method CreateOptsFile(int argc, char *argv[], char *fullprogname)

```
....
5494.             fprintf(fp, " \"%s\"", argv[i]);
```

Improper Resource Access Authorization\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2416
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5794	5794
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method defaultNoticeProcessor(void *arg, const char *message)

```
....
5794.       fprintf(stderr, "%s", message);
```

Improper Resource Access Authorization\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2417
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5879	5879

Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5879.               fprintf(stderr,
```

Improper Resource Access Authorization\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2418
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5888	5888
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5888.               fprintf(stderr,
```

Improper Resource Access Authorization\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2419
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	1215	1215
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
1215.                   fprintf(fpidfile, "%d\n", MyProcPid);
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2420
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5571	5571
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method CreateOptsFile(int argc, char *argv[], char *fullprogname)

```
....
5571.       fprintf(fp, "%s", fullprogname);
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2421
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5573	5573
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method CreateOptsFile(int argc, char *argv[], char *fullprogname)

```
....
5573.            fprintf(fp, " \"%s\"", argv[i]);
```

Improper Resource Access Authorization\Path 30:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2422
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5797	5797
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method defaultNoticeProcessor(void *arg, const char *message)

```
....
5797.       fprintf(stderr, "%s", message);
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2423
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5880	5880
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5880.             fprintf(stderr,
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2424
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5889	5889
Object	fprintf	fprintf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5889.             fprintf(stderr,
```

Improper Resource Access Authorization\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2425
Status New

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	1934	1934
Object	fprintf	fprintf

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static void standalone_main(void) {

```
....
1934.      fprintf(stderr, "error opening PidFile '%s': %s\n",
pr_pidfile_get(),
```

Improper Resource Access Authorization\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2426
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	193	193

Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
193.                fprintf(stderr, "create directory %s failed, %s\n",
path_c, strerror(errno));
```

Improper Resource Access Authorization\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2427
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	656	656
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_list_dir(const char *path, list_callback callback, void *userptr)

```
....
656.            fprintf(stderr, "open directory failed, %s\n",
strerror(errno));
```

Improper Resource Access Authorization\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2428
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	766	766
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Method	static int _tlog_remove_oldlog(struct tlog_log *log)

```
....
766.          fprintf(stderr, "get log file count failed.\n");
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2429
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	803	803
Object	fprintf	fprintf

Code Snippet

File Name	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method	static int _tlog_log_lock(struct tlog_log *log)

```
....
803.          fprintf(stderr, "create pid file failed, %s",
strerror(errno));
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2430
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1051	1051
Object	fprintf	fprintf

Code Snippet

File Name	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method	static int _tlog_write(struct tlog_log *log, char *buff, int bufflen)

```
....
1051.              fprintf(stderr, "create log dir %s failed.\n", log-
>logdir);
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2431
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1062	1062
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, char *buff, int bufflen)

```
....
1062.               fprintf(stderr, "open log file %s failed, %s\n",
logfile, strerror(errno));
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2432
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1500	1500
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1500.           fprintf(stderr, "tlog is not initialized.");
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2433
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1506	1506
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1506.           fprintf(stderr, "malloc log failed.");
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2434
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1546	1546
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1546.           fprintf(stderr, "malloc log buffer failed, %s\n",
strerror(errno));
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2435
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1588	1588
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1588.           fprintf(stderr, "tlog already initilized.\n");
```

Improper Resource Access Authorization\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2436
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1593	1593
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1593.           fprintf(stderr, "buffer size is invalid.\n");
```

Improper Resource Access Authorization\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2437
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c

Line	1609	1609
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1609.           fprintf(stderr, "init tlog root failed.\n");
```

Improper Resource Access Authorization\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2438
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1616	1616
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1616.           fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Improper Resource Access Authorization\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2439
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	193	193
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
193.              fprintf(stderr, "create directory %s failed, %s\n",
path_c, strerror(errno));
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2440
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	656	656
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_list_dir(const char *path, list_callback callback, void *userptr)

```
....
656.          fprintf(stderr, "open directory failed, %s\n",
strerror(errno));
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2441
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	766	766
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_remove_oldlog(struct tlog_log *log)

```
....
766.          fprintf(stderr, "get log file count failed.\n");
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2442
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	803	803
Object	fprintf	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
803.          fprintf(stderr, "create pid file failed, %s",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:
CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2711
Status	New

The system data read by daemonize in the file proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c at line 1764 is potentially exposed by daemonize found in proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c at line 1764.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	1773	1773

Object	perror	perror

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static void daemonize(void) {

```
....
1773.         perror("fork(2) error");
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2712
Status	New

The system data read by daemonize in the file proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c at line 1781 is potentially exposed by daemonize found in proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c at line 1781.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	1792	1792
Object	perror	perror

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static int daemonize(void) {

```
....
1792.         perror("fork(2) error");
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2713
Status	New

The system data read by standalone_main in the file proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c at line 1883 is potentially exposed by standalone_main found in proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c at line 1883.

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	1935	1934

Object	errno	fprintf

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static void standalone_main(void) {

```
....
1935.         strerror(errno));
....
1934.       fprintf(stderr, "error opening PidFile '%s': %s\n",
pr_pidfile_get(),
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2714
Status New

The system data read by _tlog_mkdir in the file pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 160 is potentially exposed by _tlog_mkdir found in pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 160.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	193	193
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
193.               fprintf(stderr, "create directory %s failed, %s\n",
path_c, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2715
Status New

The system data read by _tlog_list_dir in the file pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 648 is potentially exposed by _tlog_list_dir found in pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 648.

	Source	Destination

File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	656	656
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_list_dir(const char *path, list_callback callback, void *userptr)

```
....
656.          fprintf(stderr, "open directory failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2716
Status New

The system data read by _tlog_log_lock in the file pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 791 is potentially exposed by _tlog_log_lock found in pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 791.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	803	803
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
803.          fprintf(stderr, "create pid file failed, %s",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2717
Status New

The system data read by _tlog_write in the file pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 1008 is potentially exposed by _tlog_write found in pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 1008.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1062	1062
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, char *buff, int bufflen)

```
....
1062.               fprintf(stderr, "open log file %s failed, %s\n",
logfile, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2718
Status New

The system data read by *tlog_open in the file pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 1494 is potentially exposed by *tlog_open found in pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 1494.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1546	1546
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1546.           fprintf(stderr, "malloc log buffer failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2719
Status New

The system data read by tlog_init in the file pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 1581 is potentially exposed by tlog_init found in pymumu@@smartdns-Release31-CVE-2024-24198-TP.c at line 1581.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1616	1616
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1616.           fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2720
Status New

The system data read by _tlog_mkdir in the file pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 160 is potentially exposed by _tlog_mkdir found in pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 160.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	193	193
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
193.               fprintf(stderr, "create directory %s failed, %s\n",
path_c, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2721
Status	New

The system data read by _tlog_list_dir in the file pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 648 is potentially exposed by _tlog_list_dir found in pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 648.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	656	656
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_list_dir(const char *path, list_callback callback, void *userptr)

```
....
656.          fprintf(stderr, "open directory failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2722
Status	New

The system data read by _tlog_log_lock in the file pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 791 is potentially exposed by _tlog_log_lock found in pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 791.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	803	803
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
803.          fprintf(stderr, "create pid file failed, %s",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2723
Status	New

The system data read by _tlog_write in the file pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 1008 is potentially exposed by _tlog_write found in pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 1008.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1062	1062
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, char *buff, int bufflen)

```
....
1062.               fprintf(stderr, "open log file %s failed, %s\n",
logfile, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2724
Status	New

The system data read by *tlog_open in the file pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 1494 is potentially exposed by *tlog_open found in pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 1494.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1546	1546
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1546.          fprintf(stderr, "malloc log buffer failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2725
Status	New

The system data read by tlog_init in the file pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 1581 is potentially exposed by tlog_init found in pymumu@@smartdns-Release31-CVE-2024-24199-TP.c at line 1581.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1616	1616
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1616.          fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2726
Status	New

The system data read by _tlog_mkdir in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 160 is potentially exposed by _tlog_mkdir found in pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 160.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	202	202
Object	errno	fprintf

Code Snippet	
File Name	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method	static int _tlog_mkdir(const char *path)

```
....
202.                fprintf(stderr, "create directory %s failed, %s\n",
path_c, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2727
Status	New

The system data read by _tlog_list_dir in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 664 is potentially exposed by _tlog_list_dir found in pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 664.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	673	673
Object	errno	fprintf

Code Snippet	
File Name	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method	static int _tlog_list_dir(const char *path, list_callback callback, void *userptr)

```
....
673.            fprintf(stderr, "open directory failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2728
Status	New

The system data read by _tlog_log_lock in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 809 is potentially exposed by _tlog_log_lock found in pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 809.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c

Line	821	821
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
821.          fprintf(stderr, "create pid file failed, %s",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2729
Status	New

The system data read by _tlog_write in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 1026 is potentially exposed by _tlog_write found in pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 1026.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1081	1081
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1081.              fprintf(stderr, "open log file %s failed, %s\n",
logfile, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2730
Status	New

The system data read by *tlog_open in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 1521 is potentially exposed by *tlog_open found in pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 1521.

	Source	Destination

File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1573	1573
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1573.           fprintf(stderr, "malloc log buffer failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2731
Status New

The system data read by tlog_init in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 1608 is potentially exposed by tlog_init found in pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c at line 1608.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1643	1643
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1643.           fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2732
Status New

The system data read by _tlog_mkdir in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 160 is potentially exposed by _tlog_mkdir found in pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 160.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	202	202
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
202.              fprintf(stderr, "create directory %s failed, %s\n",
path_c, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2733
Status New

The system data read by _tlog_list_dir in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 664 is potentially exposed by _tlog_list_dir found in pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 664.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	673	673
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static int _tlog_list_dir(const char *path, list_callback callback, void *userptr)

```
....
673.          fprintf(stderr, "open directory failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=2734
Status	New

The system data read by _tlog_log_lock in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 809 is potentially exposed by _tlog_log_lock found in pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 809.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	821	821
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
821.          fprintf(stderr, "create pid file failed, %s",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2735
Status	New

The system data read by _tlog_write in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 1026 is potentially exposed by _tlog_write found in pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 1026.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	1081	1081
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1081.              fprintf(stderr, "open log file %s failed, %s\n",
logfile, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 26:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2736
Status	New

The system data read by *tlog_open in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 1521 is potentially exposed by *tlog_open found in pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 1521.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	1573	1573
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1573.           fprintf(stderr, "malloc log buffer failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2737
Status	New

The system data read by tlog_init in the file pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 1608 is potentially exposed by tlog_init found in pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c at line 1608.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	1643	1643
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1643.          fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2738
Status	New

The system data read by _tlog_mkdir in the file pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 168 is potentially exposed by _tlog_mkdir found in pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 168.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	210	210
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
210.              fprintf(stderr, "create directory %s failed, %s\n",
path_c, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2739
Status	New

The system data read by _tlog_list_dir in the file pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 700 is potentially exposed by _tlog_list_dir found in pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 700.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	709	709
Object	errno	fprintf

Code Snippet	
File Name	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method	static int _tlog_list_dir(const char *path, list_callback callback, void *userptr)

```
....
709.            fprintf(stderr, "open directory failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2740
Status	New

The system data read by _tlog_log_lock in the file pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 845 is potentially exposed by _tlog_log_lock found in pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 845.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	857	857
Object	errno	fprintf

Code Snippet	
File Name	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method	static int _tlog_log_lock(struct tlog_log *log)

```
....
857.            fprintf(stderr, "create pid file failed, %s",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2741
Status	New

The system data read by _tlog_write in the file pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 1082 is potentially exposed by _tlog_write found in pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 1082.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1142	1142

Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1142.              fprintf(stderr, "open log file %s failed, %s\n",
logfile, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2742
Status New

The system data read by *tlog_open in the file pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 1585 is potentially exposed by *tlog_open found in pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 1585.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1633	1633
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1633.          fprintf(stderr, "malloc log buffer failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2743
Status New

The system data read by tlog_fork_child in the file pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 1694 is potentially exposed by tlog_fork_child found in pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 1694.

	Source	Destination

File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1705	1705
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static void tlog_fork_child(void)

```
....
1705.           fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2744
Status New

The system data read by tlog_init in the file pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 1720 is potentially exposed by tlog_init found in pymumu@@smartdns-Release34-CVE-2024-24198-TP.c at line 1720.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1755	1755
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1755.           fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2745
Status New

The system data read by _tlog_mkdir in the file pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 168 is potentially exposed by _tlog_mkdir found in pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 168.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	210	210
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
210.              fprintf(stderr, "create directory %s failed, %s\n",
path_c, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2746
Status New

The system data read by _tlog_list_dir in the file pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 700 is potentially exposed by _tlog_list_dir found in pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 700.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	709	709
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static int _tlog_list_dir(const char *path, list_callback callback, void *userptr)

```
....
709.          fprintf(stderr, "open directory failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=2747
Status	New

The system data read by _tlog_log_lock in the file pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 845 is potentially exposed by _tlog_log_lock found in pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 845.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	857	857
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
857.          fprintf(stderr, "create pid file failed, %s",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2748
Status	New

The system data read by _tlog_write in the file pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 1082 is potentially exposed by _tlog_write found in pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 1082.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1142	1142
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1142.              fprintf(stderr, "open log file %s failed, %s\n",
logfile, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 39:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2749
Status	New

The system data read by *tlog_open in the file pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 1585 is potentially exposed by *tlog_open found in pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 1585.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1633	1633
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1633.           fprintf(stderr, "malloc log buffer failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2750
Status	New

The system data read by tlog_fork_child in the file pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 1694 is potentially exposed by tlog_fork_child found in pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 1694.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1705	1705
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static void tlog_fork_child(void)

```
....
1705.          fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2751
Status	New

The system data read by tlog_init in the file pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 1720 is potentially exposed by tlog_init found in pymumu@@smartdns-Release34-CVE-2024-24199-TP.c at line 1720.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1755	1755
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1755.          fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2752
Status	New

The system data read by _tlog_mkdir in the file pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 168 is potentially exposed by _tlog_mkdir found in pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 168.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	210	210
Object	errno	fprintf

Code Snippet	
File Name	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method	static int _tlog_mkdir(const char *path)

```
....
210.              fprintf(stderr, "create directory %s failed, %s\n",
path_c, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2753
Status	New

The system data read by _tlog_list_dir in the file pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 700 is potentially exposed by _tlog_list_dir found in pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 700.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	709	709
Object	errno	fprintf

Code Snippet	
File Name	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method	static int _tlog_list_dir(const char *path, list_callback callback, void *userptr)

```
....
709.          fprintf(stderr, "open directory failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2754
Status	New

The system data read by _tlog_log_lock in the file pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 845 is potentially exposed by _tlog_log_lock found in pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 845.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c

Line	857	857
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
857.          fprintf(stderr, "create pid file failed, %s",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2755
Status	New

The system data read by _tlog_write in the file pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 1082 is potentially exposed by _tlog_write found in pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 1082.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1142	1142
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1142.              fprintf(stderr, "open log file %s failed, %s\n",
logfile, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2756
Status	New

The system data read by *tlog_open in the file pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 1617 is potentially exposed by *tlog_open found in pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 1617.

	Source	Destination

File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1665	1665
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method tlog_log *tlog_open(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1665.           fprintf(stderr, "malloc log buffer failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2757
Status	New

The system data read by tlog_fork_child in the file pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 1732 is potentially exposed by tlog_fork_child found in pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 1732.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1753	1753
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static void tlog_fork_child(void)

```
....
1753.           fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2758
Status	New

The system data read by tlog_init in the file pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 1768 is potentially exposed by tlog_init found in pymumu@@smartdns-Release36-CVE-2024-24198-TP.c at line 1768.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1803	1803
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1803.           fprintf(stderr, "create tlog work thread failed, %s\n",
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2759
Status New

The system data read by _tlog_mkdir in the file pymumu@@smartdns-Release36-CVE-2024-24199-TP.c at line 168 is potentially exposed by _tlog_mkdir found in pymumu@@smartdns-Release36-CVE-2024-24199-TP.c at line 168.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	210	210
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
210.                fprintf(stderr, "create directory %s failed, %s\n",
path_c, strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2760
Status	New

The system data read by _tlog_list_dir in the file pymumu@@smartdns-Release36-CVE-2024-24199-TP.c at line 700 is potentially exposed by _tlog_list_dir found in pymumu@@smartdns-Release36-CVE-2024-24199-TP.c at line 700.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	709	709
Object	errno	fprintf

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static int _tlog_list_dir(const char *path, list_callback callback, void *userptr)

```
....
709.          fprintf(stderr, "open directory failed, %s\n",
strerror(errno));
```

Unreleased Resource Leak

Query Path:
CPP\Cx\CPP Low Visibility\Unreleased Resource Leak Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Unreleased Resource Leak\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3301
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1603	1603
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1603.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3302
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1603	1603
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1603.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3303
Status	New

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1630	1630
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1630.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3304
Status	New

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	1630	1630
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1630.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3305
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1742	1742
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1742.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=3306
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1742	1742
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1742.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3307
Status	New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1790	1790
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1790.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3308
Status	New

	Source	Destination

File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	1790	1790
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1790.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3309
Status New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	1822	1822
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1822.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3310
Status New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	1822	1822

Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1822.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3311
Status New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	1858	1858
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1858.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3312
Status New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Line	1858	1858
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c

Method	int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1858.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3313
Status	New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Line	1863	1863
Object	tlog	tlog

Code Snippet	
File Name	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Method	int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1863.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3314
Status	New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Line	1863	1863
Object	tlog	tlog

Code Snippet	
File Name	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Method	int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1863.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3315
Status	New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Line	1935	1935
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1935.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3316
Status	New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Line	1935	1935
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1935.       pthread_cond_init(&tlog.cond, NULL);
```

Unreleased Resource Leak\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3317
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	6080	6080
Object	singlethread_lock	singlethread_lock

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method default_threadlock(int acquire)

```
....
6080.             if (pthread_mutex_lock(&singlethread_lock))
```

Unreleased Resource Leak\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3318
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	6099	6099
Object	singlethread_lock	singlethread_lock

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method default_threadlock(int acquire)

```
....
6099.             if (pthread_mutex_lock(&singlethread_lock))
```

Unreleased Resource Leak\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3319
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1682	1682
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static void tlog_fork_prepare(void)

```
....
1682.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3320
Status New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1682	1682
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static void tlog_fork_prepare(void)

```
....
1682.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3321
Status New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1714	1714

Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static void tlog_fork_prepare(void)

```
....
1714.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3322
Status New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	1714	1714
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static void tlog_fork_prepare(void)

```
....
1714.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3323
Status New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	1746	1746
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method static void tlog_fork_prepare(void)

```
....
1746.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3324
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	1746	1746
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method static void tlog_fork_prepare(void)

```
....
1746.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3325
Status	New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	1782	1782
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method static void tlog_fork_prepare(void)

```
....
1782.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 26:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3326
Status	New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Line	1782	1782
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Method static void tlog_fork_prepare(void)

```
....
1782.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3327
Status	New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Line	1787	1787
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Method static void tlog_fork_prepare(void)

```
....
1787.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3328
Status	New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Line	1787	1787
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Method static void tlog_fork_prepare(void)

```
....
1787.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3329
Status New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Line	1858	1858
Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Method static void tlog_fork_prepare(void)

```
....
1858.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3330
Status New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Line	1858	1858

Object	tlog	tlog

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Method static void tlog_fork_prepare(void)

```
....
1858.       pthread_mutex_lock(&tlog.lock);
```

Unreleased Resource Leak\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3331
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1602	1602
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1602.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3332
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1602	1602
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c

Method	int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1602.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3333
Status	New

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1629	1629
Object	attr	attr

Code Snippet	
File Name	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method	int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1629.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3334
Status	New

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	1629	1629
Object	attr	attr

Code Snippet	
File Name	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method	int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1629.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3335
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1702	1702
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static void tlog_fork_child(void)

```
....
1702.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3336
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1741	1741
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1741.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3337
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1702	1702
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static void tlog_fork_child(void)

```
....
1702.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3338
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1741	1741
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1741.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3339
Status	New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1750	1750
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static void tlog_fork_child(void)

```
....
1750.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3340
Status New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1789	1789
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1789.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3341
Status New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c

Line	1750	1750
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static void tlog_fork_child(void)

```
....
1750.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3342
Status New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	1789	1789
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1789.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3343
Status New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	1782	1782
Object	attr	attr

Code Snippet

File Name	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method	static void tlog_fork_child(void)

```
....
1782.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3344
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	1821	1821
Object	attr	attr

Code Snippet

File Name	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method	int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1821.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3345
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	1782	1782
Object	attr	attr

Code Snippet

File Name	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method	static void tlog_fork_child(void)

```
....
1782.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3346
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	1821	1821
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1821.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3347
Status	New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	1818	1818
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method static void tlog_fork_child(void)

```
....
1818.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=3348
Status	New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	1857	1857
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1857.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3349
Status	New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Line	1818	1818
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Method static void tlog_fork_child(void)

```
....
1818.       pthread_attr_init(&attr);
```

Unreleased Resource Leak\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3350
Status	New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-	pymumu@@smartdns-Release38.1-CVE-

	2024-24199-TP.c	2024-24199-TP.c
Line	1857	1857
Object	attr	attr

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Method int tlog_init(const char *logfile, int maxlogsize, int maxlogcount, int buffsize, unsigned int flag)

```
....
1857.       pthread_attr_init(&attr);
```

TOCTOU

Query Path:
CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2824
Status	New

The openQueryOutputFile method in postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Line	62	62
Object	fopen	fopen

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25696-TP.c
Method openQueryOutputFile(const char *fname, FILE **fout, bool *is_pipe)

```
....
62.          *fout = fopen(fname, "w");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2825
Status	New

The PostmasterMain method in postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	1192	1192
Object	fopen	fopen

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
1192.             FILE     *fpidfile = fopen(external_pid_file, "w");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2826
Status	New

The CreateOptsFile method in postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5486	5486
Object	fopen	fopen

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method CreateOptsFile(int argc, char *argv[], char *fullprogname)

```
....
5486.       if ((fp = fopen(OPTS_FILE, "w")) == NULL)
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2827
Status	New

The parseServiceFile method in postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	4079	4079
Object	fopen	fopen

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method parseServiceFile(const char *serviceFile,

```
....
4079.       f = fopen(serviceFile, "r");
```

TOCTOU\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2828
Status New

The PasswordFromFile method in postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5901	5901
Object	fopen	fopen

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5901.       fp = fopen(pgpassfile, "r");
```

TOCTOU\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2829

Status	New

The PostmasterMain method in postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	1211	1211
Object	fopen	fopen

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
1211.             FILE     *fpidfile = fopen(external_pid_file, "w");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2830
Status	New

The CreateOptsFile method in postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5565	5565
Object	fopen	fopen

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method CreateOptsFile(int argc, char *argv[], char *fullprogname)

```
....
5565.       if ((fp = fopen(OPTS_FILE, "w")) == NULL)
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=2831
Status	New

The parseServiceFile method in postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	4082	4082
Object	fopen	fopen

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method parseServiceFile(const char *serviceFile,

```
....
4082.       f = fopen(serviceFile, "r");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2832
Status	New

The PasswordFromFile method in postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5902	5902
Object	fopen	fopen

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5902.       fp = fopen(pgpassfile, "r");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2833
Status	New

The show_os_release method in proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	2059	2059
Object	fopen	fopen

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void show_os_release(void) {

```
....
2059.     fh = fopen(os_release_path, "r");
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2834
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release31-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	801	801
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
801.       fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 12:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2835
Status	New

The _tlog_write method in pymumu@@smartdns-Release31-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	1056	1056
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, char *buff, int bufflen)

```
....
1056.           log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, 0640);
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2836
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release31-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	801	801
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
801.       fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2837
Status	New

The _tlog_write method in pymumu@@smartdns-Release31-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	1056	1056
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, char *buff, int bufflen)

```
....
1056.          log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, 0640);
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2838
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	819	819
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
819.        fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2839
Status	New

The _tlog_write method in pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	1075	1075
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1075.           log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, 0640);
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2840
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	819	819
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
819.       fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2841
Status	New

The _tlog_write method in pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	1075	1075
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1075.           log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, 0640);
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2842
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release34-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	855	855

Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
855.       fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2843
Status	New

The _tlog_write method in pymumu@@smartdns-Release34-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	1136	1136
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1136.           log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2844
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release34-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-	pymumu@@smartdns-Release34-CVE-

	2024-24199-TP.c	2024-24199-TP.c
Line	855	855
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
855.       fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2845
Status	New

The _tlog_write method in pymumu@@smartdns-Release34-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	1136	1136
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1136.           log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2846
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release36-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	855	855
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
855.      fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2847
Status	New

The _tlog_write method in pymumu@@smartdns-Release36-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	1136	1136
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1136.          log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2848
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release36-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	855	855
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
855.       fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2849
Status	New

The _tlog_write method in pymumu@@smartdns-Release36-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	1136	1136
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1136.           log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=2850
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	867	867
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
867.      fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2851
Status	New

The _tlog_close_all_fd method in pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	955	955
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method static void _tlog_close_all_fd(void)

```
....
955.      dir_fd = open("/proc/self/fd/", O_RDONLY | O_DIRECTORY);
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2852
Status	New

The _tlog_write method in pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	1168	1168
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1168.           log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2853
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	867	867
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
867.       fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2854
Status	New

The _tlog_close_all_fd method in pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	955	955
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method static void _tlog_close_all_fd(void)

```
....
955.      dir_fd = open("/proc/self/fd/", O_RDONLY | O_DIRECTORY);
```

TOCTOU\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2855
Status	New

The _tlog_write method in pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	1168	1168
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1168.          log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2856
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	867	867
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
867.      fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2857
Status	New

The _tlog_close_all_fd method in pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	955	955
Object	open	open

Code Snippet	
File Name	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method	static void _tlog_close_all_fd(void)

```
....
955.      dir_fd = open("/proc/self/fd/", O_RDONLY | O_DIRECTORY);
```

TOCTOU\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2858
Status	New

The _tlog_write method in pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	1180	1180
Object	open	open

Code Snippet	
File Name	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method	static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1180.          log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2859
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Line	867	867

Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
867.      fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2860
Status New

The _tlog_close_all_fd method in pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Line	955	955
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Method static void _tlog_close_all_fd(void)

```
....
955.      dir_fd = open("/proc/self/fd/", O_RDONLY | O_DIRECTORY);
```

TOCTOU\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2861
Status New

The _tlog_write method in pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c

Line	1180	1180
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1180.          log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2862
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Line	886	886
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
886.      fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2863
Status	New

The _tlog_close_all_fd method in pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Line	974	974
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Method static void _tlog_close_all_fd(void)

```
....
974.      dir_fd = open("/proc/self/fd/", O_RDONLY | O_DIRECTORY);
```

TOCTOU\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2864
Status	New

The _tlog_write method in pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Line	1199	1199
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1199.          log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2865
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Line	886	886
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
886.      fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2866
Status New

The _tlog_close_all_fd method in pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Line	974	974
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Method static void _tlog_close_all_fd(void)

```
....
974.      dir_fd = open("/proc/self/fd/", O_RDONLY | O_DIRECTORY);
```

TOCTOU\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2867
Status New

The _tlog_write method in pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Line	1199	1199
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1199.           log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2868
Status New

The _tlog_log_lock method in pymumu@@smartdns-Release43-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Line	897	897
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
897.       fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20

	047&pathid=2869
Status	New

The _tlog_close_all_fd method in pymumu@@smartdns-Release43-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Line	985	985
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Method static void _tlog_close_all_fd(void)

```
....
985.      dir_fd = open("/proc/self/fd/", O_RDONLY | O_DIRECTORY);
```

TOCTOU\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2870
Status	New

The _tlog_write method in pymumu@@smartdns-Release43-CVE-2024-24198-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Line	1214	1214
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1214.          log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

TOCTOU\Path 48:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2871
Status	New

The _tlog_log_lock method in pymumu@@smartdns-Release43-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Line	897	897
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Method static int _tlog_log_lock(struct tlog_log *log)

```
....
897.      fd = open(lock_file, O_RDWR | O_CREAT | O_CLOEXEC, S_IRUSR |
S_IWUSR);
```

TOCTOU\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2872
Status	New

The _tlog_close_all_fd method in pymumu@@smartdns-Release43-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Line	985	985
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Method static void _tlog_close_all_fd(void)

```
....
985.      dir_fd = open("/proc/self/fd/", O_RDONLY | O_DIRECTORY);
```

TOCTOU\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2873
Status	New

The _tlog_write method in pymumu@@smartdns-Release43-CVE-2024-24199-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Line	1214	1214
Object	open	open

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Method static int _tlog_write(struct tlog_log *log, const char *buff, int bufflen)

```
....
1214.          log->fd = open(logfile, O_APPEND | O_CREAT | O_WRONLY |
O_CLOEXEC, log->file_perm);
```

Incorrect Permission Assignment For Critical Resources

Query Path:
CPP\Cx\CPP Low Visibility\Incorrect Permission Assignment For Critical Resources Version:1

Categories

FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description
Incorrect Permission Assignment For Critical Resources\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2670
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	1200	1200
Object	chmod	chmod

Code Snippet

File Name	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method	PostmasterMain(int argc, char *argv[])

```
....
1200.                   if (chmod(external_pid_file, S_IRUSR | S_IWUSR |
S_IRGRP | S_IROTH) != 0)
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2671
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	1219	1219
Object	chmod	chmod

Code Snippet

File Name	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method	PostmasterMain(int argc, char *argv[])

```
....
1219.                   if (chmod(external_pid_file, S_IRUSR | S_IWUSR |
S_IRGRP | S_IROTH) != 0)
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2672
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	695	695
Object	chmod	chmod

Code Snippet

File Name	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method	static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
695.      chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2673
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	695	695
Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
695.      chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2674
Status	New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	695	695
Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
695.      chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2675
Status	New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	695	695
Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
695.      chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2676
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	707	707
Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
707.      chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2677
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	707	707
Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
707.        chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2678
Status New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	707	707
Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
707.        chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2679
Status New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Line	707	707

Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
707.      chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2680
Status New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Line	726	726
Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
726.      chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2681
Status New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Line	726	726
Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
726.      chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2682
Status	New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Line	737	737
Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
737.      chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2683
Status	New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Line	737	737
Object	chmod	chmod

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Method static int _tlog_rename_logfile(struct tlog_log *log, const char *log_file)

```
....
737.      chmod(archive_file, log->archive_perm);
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2684
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5486	5486
Object	fp	fp

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method CreateOptsFile(int argc, char *argv[], char *fullprogname)

```
....
5486.       if ((fp = fopen(OPTS_FILE, "w")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2685
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	4079	4079
Object	f	f

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method parseServiceFile(const char *serviceFile,

```
....
4079.       f = fopen(serviceFile, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2686
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	5901	5901
Object	fp	fp

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5901.       fp = fopen(pgpassfile, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2687
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5565	5565
Object	fp	fp

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method CreateOptsFile(int argc, char *argv[], char *fullprogname)

```
....
5565.       if ((fp = fopen(OPTS_FILE, "w")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2688
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	4082	4082

Object	f	f

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method parseServiceFile(const char *serviceFile,

```
....
4082.       f = fopen(serviceFile, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2689
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	5902	5902
Object	fp	fp

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PasswordFromFile(char *hostname, char *port, char *dbname, char *username)

```
....
5902.       fp = fopen(pgpassfile, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2690
Status New

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	2059	2059
Object	fh	fh

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void show_os_release(void) {

```
....
2059.    fh = fopen(os_release_path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2691
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	1192	1192
Object	fpidfile	fpidfile

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
1192.            FILE     *fpidfile = fopen(external_pid_file, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2692
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	1211	1211
Object	fpidfile	fpidfile

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
1211.            FILE     *fpidfile = fopen(external_pid_file, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 24:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2693
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4431	4431
Object	mkdir	mkdir

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method internal_forkexec(int argc, char *argv[], Port *port)

```
....
4431.             mkdir(PG_TEMP_FILES_DIR, S_IRWXU);
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2694
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	4467	4467
Object	mkdir	mkdir

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method internal_forkexec(int argc, char *argv[], Port *port)

```
....
4467.             mkdir(PG_TEMP_FILES_DIR, S_IRWXU);
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2695
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	192	192
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
192.            if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2696
Status New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	192	192
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
192.            if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2697
Status New

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	201	201

Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
201.          if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2698
Status New

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	201	201
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
201.          if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2699
Status New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	209	209
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
209.          if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2700
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	209	209
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
209.          if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2701
Status	New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	209	209
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
209.          if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 33:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2702
Status	New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	209	209
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
209.            if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2703
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	218	218
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
218.            if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2704
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	218	218
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
218.            if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2705
Status New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	219	219
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
219.            if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2706
Status New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Line	219	219

Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
219.          if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2707
Status New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Line	220	220
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
220.          if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2708
Status New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Line	220	220
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
220.          if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2709
Status	New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Line	221	221
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
221.          if (mkdir(path_c, 0750) != 0) {
```

Incorrect Permission Assignment For Critical Resources\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2710
Status	New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Line	221	221
Object	mkdir	mkdir

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
221.          if (mkdir(path_c, 0750) != 0) {
```

Unchecked Array Index

Query Path:

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unchecked Array Index\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3375
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4392	4392
Object	ac	ac

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method backend_forkexec(Port *port)

```
....
4392.        av[ac] = NULL;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3376
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5292	5292
Object	ac	ac

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method StartChildProcess(AuxProcType type)

```
....
5292.        av[ac] = NULL;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3377
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5599	5599
Object	ac	ac

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method bgworker_forkexec(int shmem_slot)

```
....
5599.       av[ac] = NULL;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3378
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	6303	6303
Object	i	i

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method ShmemBackendArrayAdd(Backend *bn)

```
....
6303.       ShmemBackendArray[i] = *bn;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3379
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	4428	4428
Object	ac	ac

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method backend_forkexec(Port *port)

```
....
4428.       av[ac] = NULL;
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3380
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5371	5371
Object	ac	ac

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method StartChildProcess(AuxProcType type)

```
....
5371.       av[ac] = NULL;
```

Unchecked Array Index\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3381
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5678	5678

Object	ac	ac

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method bgworker_forkexec(int shmem_slot)

```
....
5678.        av[ac] = NULL;
```

Unchecked Array Index\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3382
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	6381	6381
Object	i	i

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method ShmemBackendArrayAdd(Backend *bn)

```
....
6381.        ShmemBackendArray[i] = *bn;
```

Unchecked Array Index\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3383
Status New

	Source	Destination
File	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c	pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Line	68	68
Object	SID_SIZE	SID_SIZE

Code Snippet
File Name pupnp@@pupnp-release-1.8.7-CVE-2020-13848-FP.c
Method copy_subscription(subscription * in,

```
....
68.      out->sid[SID_SIZE] = 0;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3384
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c	pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Line	173	173
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
173.      path_c[len] = '/';
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3385
Status	New

	Source	Destination
File	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c	pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Line	173	173
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release31-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
173.      path_c[len] = '/';
```

Unchecked Array Index\Path 12:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3386
Status	New

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Line	177	177
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
177.        path_c[len] = '/';
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3387
Status	New

	Source	Destination
File	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c	pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Line	177	177
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release32-RC2-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
177.        path_c[len] = '/';
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3388
Status	New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c	pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Line	185	185
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
185.        path_c[len] = '/';
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3389
Status New

	Source	Destination
File	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c	pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Line	185	185
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release34-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
185.        path_c[len] = '/';
```

Unchecked Array Index\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3390
Status New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c	pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Line	185	185

Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
185.        path_c[len] = '/';
```

Unchecked Array Index\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3391
Status New

	Source	Destination
File	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c	pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Line	185	185
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release36-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
185.        path_c[len] = '/';
```

Unchecked Array Index\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3392
Status New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Line	194	194
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
194.      path_c[len] = '/';
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3393
Status	New

	Source	Destination
File	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Line	194	194
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release37-RC1-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
194.      path_c[len] = '/';
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3394
Status	New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Line	195	195
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
195.      path_c[len] = '/';
```

Unchecked Array Index\Path 21:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3395
Status	New

	Source	Destination
File	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Line	195	195
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release38.1-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
195.        path_c[len] = '/';
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3396
Status	New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Line	196	196
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
196.        path_c[len] = '/';
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3397
Status	New

	Source	Destination
File	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c	pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Line	196	196
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release41-RC1-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
196.        path_c[len] = '/';
```

Unchecked Array Index\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3398
Status New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c	pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Line	197	197
Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24198-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
197.        path_c[len] = '/';
```

Unchecked Array Index\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3399
Status New

	Source	Destination
File	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c	pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Line	197	197

Object	len	len

Code Snippet
File Name pymumu@@smartdns-Release43-CVE-2024-24199-TP.c
Method static int _tlog_mkdir(const char *path)

```
....
197.      path_c[len] = '/';
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3284
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	3009	4219
Object	SetConstraintState	sizeof

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method typedef SetConstraintStateData *SetConstraintState;

```
....
3009.  typedef SetConstraintStateData *SetConstraintState;
```

File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method AfterTriggerBeginSubXact(void)

```
....
4219.                                        new_alloc *
sizeof(SetConstraintState));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3285
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	3009	4201
Object	SetConstraintState	sizeof

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method typedef SetConstraintStateData *SetConstraintState;

```
....
3009.  typedef SetConstraintStateData *SetConstraintState;
```

File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method AfterTriggerBeginSubXact(void)

```
....
4201.                          palloc(DEFTRIG_INITALLOC *
sizeof(SetConstraintState));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3286
Status New

	Source	Destination
File	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Line	3490	3534
Object	GenericHandler	sizeof

Code Snippet
File Name protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Method typedef void (*GenericHandler) (void *service,

```
....
3490.  typedef void (*GenericHandler) (void *service,
```

File Name protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3534.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3287
Status	New

	Source	Destination
File	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Line	3497	3541
Object	GenericHandler	sizeof

Code Snippet

File Name protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c

Method typedef void (*GenericHandler) (void *service,

```
....
3497.  typedef void (*GenericHandler) (void *service,
```

File Name protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c

Method protobuf_c_service_generated_init(ProtobufCService *service,

```
....
3541.       memset(service + 1, 0, descriptor->n_methods *
sizeof(GenericHandler));
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3288
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	1578	1578
Object	sizeof	sizeof

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method RelationBuildTriggers(Relation relation)

```
....
1578.                   build->tgargs = (char **) palloc(build->tgnargs
* sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3289
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	1725	1725
Object	sizeof	sizeof

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method CopyTriggerDesc(TriggerDesc *trigdesc)

```
....
1725.                   newargs = (char **) palloc(trigger->tgnargs *
sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3290
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	4379	4379
Object	sizeof	sizeof

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method AfterTriggerEnlargeQueryState(void)

```
....
4379.                                                   new_alloc *
sizeof(Tuplestorestate *));
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3291
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	4394	4394
Object	sizeof	sizeof

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method AfterTriggerEnlargeQueryState(void)

```
....
4394.                                   new_alloc * sizeof(Tuplestorestate
*));
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3292
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c	postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Line	4397	4397
Object	sizeof	sizeof

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2020-25695-TP.c
Method AfterTriggerEnlargeQueryState(void)

```
....
4397.                       0, (new_alloc - old_alloc) *
sizeof(Tuplestorestate *));
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3293
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4312	4312
Object	sizeof	sizeof

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method BackendRun(Port *port)

```
....
4312.                                                    maxac *
sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3294
Status	New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	4348	4348
Object	sizeof	sizeof

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method BackendRun(Port *port)

```
....
4348.                                                    maxac *
sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3295
Status	New

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	831	831
Object	sizeof	sizeof

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method static cmd_rec *make_ftp_cmd(pool *p, char *buf, size_t buflen, int flags) {

```
....
831.    tarr = make_array(cmd->pool, 2, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3296
Status	New

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	841	841
Object	sizeof	sizeof

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static cmd_rec *make_ftp_cmd(pool *p, char *buf, size_t buflen, int flags) {

```
....
841.    tarr = make_array(cmd->pool, 2, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3297
Status	New

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-	proftpd@@proftpd-v1.3.8-CVE-2023-

	51713-TP.c	51713-TP.c
Line	1993	1993
Object	sizeof	sizeof

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void list_directives(void) {

```
....
1993.    directives = make_array(tmp_pool, 1, sizeof(conftable **));
```

Use of Sizeof On a Pointer Type\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3298
Status New

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Line	2011	2011
Object	sizeof	sizeof

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method static void list_directives(void) {

```
....
2011.    qsort((void *) directives->elts, directives->nelts,
sizeof(conftable **),
```

Use of Sizeof On a Pointer Type\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3299
Status New

	Source	Destination
File	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Line	1256	1256
Object	sizeof	sizeof

Code Snippet
File Name protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Method sizeof_elt_in_repeated_array(ProtobufCType type)

```
....
1256.             return sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=3300
Status New

	Source	Destination
File	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Line	1260	1260
Object	sizeof	sizeof

Code Snippet
File Name protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Method sizeof_elt_in_repeated_array(ProtobufCType type)

```
....
1260.             return sizeof(void *);
```

Insufficiently Protected Credentials

Query Path:
CPP\Cx\CPP Low Visibility\Insufficiently Protected Credentials Version:0

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Insufficiently Protected Credentials\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1127
Status New

Method PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c gets a user password from the pwd element. This element's value then flows through the code without being encrypted and is written to the database in PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	1080	1169
Object	pwd	pwd

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQsetdbLogin(const char *pghost, const char *pgport, const char *pgoptions,

```
....
1080.                     const char *pwd)
....
1169.       if (pwd && pwd[0] != '\0')
```

Insufficiently Protected Credentials\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1128
Status New

Method PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c gets a user password from the pwd element. This element's value then flows through the code without being encrypted and is written to the database in PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	1080	1169
Object	pwd	pwd

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQsetdbLogin(const char *pghost, const char *pgport, const char *pgoptions,

```
....
1080.                     const char *pwd)
....
1169.       if (pwd && pwd[0] != '\0')
```

Insufficiently Protected Credentials\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1129
Status New

Method PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c gets a user password from the pwd element. This element's value then flows through the code without being encrypted and is written to the database in PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	1080	1173
Object	pwd	pwd

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQsetdbLogin(const char *pghost, const char *pgport, const char *pgoptions,

```
....
1080.                       const char *pwd)
....
1173.              conn->pgpass = strdup(pwd);
```

Insufficiently Protected Credentials\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1130
Status New

Method PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c gets a user password from the pwd element. This element's value then flows through the code without being encrypted and is written to the database in PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	1080	1169
Object	pwd	pwd

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PQsetdbLogin(const char *pghost, const char *pgport, const char *pgoptions,

```
....
1080.                       const char *pwd)
....
1169.       if (pwd && pwd[0] != '\0')
```

Insufficiently Protected Credentials\Path 5:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1131
Status	New

Method PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c gets a user password from the pwd element. This element's value then flows through the code without being encrypted and is written to the database in PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	1080	1169
Object	pwd	pwd

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PQsetdbLogin(const char *pghost, const char *pgport, const char *pgoptions,

```
....
1080.                    const char *pwd)
....
1169.       if (pwd && pwd[0] != '\0')
```

Insufficiently Protected Credentials\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1132
Status	New

Method PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c gets a user password from the pwd element. This element's value then flows through the code without being encrypted and is written to the database in PQsetdbLogin at line 1078 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	1080	1173
Object	pwd	pwd

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PQsetdbLogin(const char *pghost, const char *pgport, const char *pgoptions,

```
....
1080.                    const char *pwd)
....
1173.             conn->pgpass = strdup(pwd);
```

Insufficiently Protected Credentials\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1133
Status	New

Method PQconnectPoll at line 1738 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c gets a user password from the pwdbuf element. This element's value then flows through the code without being encrypted and is written to the database in PQconnectPoll at line 1738 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	2151	2175
Object	pwdbuf	pwdbuf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
2151.                                char        pwdbuf[BUFSIZ];
....
2175.                                passerr = pqGetpwuid(uid, &pass_buf,
pwdbuf, sizeof(pwdbuf), &pass);
```

Insufficiently Protected Credentials\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1134
Status	New

Method PQconnectPoll at line 1738 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c gets a user password from the pwdbuf element. This element's value then flows through the code without being encrypted and is written to the database in PQconnectPoll at line 1738 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	2151	2175

Object	pwdbuf	pwdbuf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
2151.                                   char        pwdbuf[BUFSIZ];
....
2175.                                   passerr = pqGetpwuid(uid, &pass_buf,
pwdbuf, sizeof(pwdbuf), &pass);
```

Insufficiently Protected Credentials\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1135
Status New

Method pqGetHomeDirectory at line 6028 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c gets a user password from the pwdbuf element. This element's value then flows through the code without being encrypted and is written to the database in pqGetHomeDirectory at line 6028 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	6031	6035
Object	pwdbuf	pwdbuf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method pqGetHomeDirectory(char *buf, int bufsize)

```
....
6031.       char        pwdbuf[BUFSIZ];
....
6035.       (void) pqGetpwuid(geteuid(), &pwdstr, pwdbuf,
sizeof(pwdbuf), &pwd);
```

Insufficiently Protected Credentials\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1136
Status New

Method pqGetHomeDirectory at line 6028 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c gets a user password from the pwdbuf element. This element's value then flows through the code without being

encrypted and is written to the database in pqGetHomeDirectory at line 6028 of postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Line	6031	6035
Object	pwdbuf	pwdbuf

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23222-TP.c
Method pqGetHomeDirectory(char *buf, int bufsize)

```
....
6031.        char        pwdbuf[BUFSIZ];
....
6035.        (void) pqGetpwuid(geteuid(), &pwdstr, pwdbuf,
sizeof(pwdbuf), &pwd);
```

Insufficiently Protected Credentials\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1137
Status New

Method PQconnectPoll at line 1738 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c gets a user password from the pwdbuf element. This element's value then flows through the code without being encrypted and is written to the database in PQconnectPoll at line 1738 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	2151	2175
Object	pwdbuf	pwdbuf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
2151.                                   char        pwdbuf[BUFSIZ];
....
2175.                                   passerr = pqGetpwuid(uid, &pass_buf,
pwdbuf, sizeof(pwdbuf), &pass);
```

Insufficiently Protected Credentials\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1138
Status	New

Method PQconnectPoll at line 1738 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c gets a user password from the pwdbuf element. This element's value then flows through the code without being encrypted and is written to the database in PQconnectPoll at line 1738 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	2151	2175
Object	pwdbuf	pwdbuf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method PQconnectPoll(PGconn *conn)

```
....
2151.                                   char        pwdbuf[BUFSIZ];
....
2175.                                   passerr = pqGetpwuid(uid, &pass_buf,
pwdbuf, sizeof(pwdbuf), &pass);
```

Insufficiently Protected Credentials\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1139
Status	New

Method pqGetHomeDirectory at line 6047 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c gets a user password from the pwdbuf element. This element's value then flows through the code without being encrypted and is written to the database in pqGetHomeDirectory at line 6047 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	6050	6054
Object	pwdbuf	pwdbuf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method pqGetHomeDirectory(char *buf, int bufsize)

```
....
6050.        char        pwdbuf[BUFSIZ];
....
6054.        (void) pqGetpwuid(geteuid(), &pwdstr, pwdbuf,
sizeof(pwdbuf), &pwd);
```

Insufficiently Protected Credentials\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1140
Status	New

Method pqGetHomeDirectory at line 6047 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c gets a user password from the pwdbuf element. This element's value then flows through the code without being encrypted and is written to the database in pqGetHomeDirectory at line 6047 of postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c. This may enable passwords to be stolen by an attacker.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Line	6050	6054
Object	pwdbuf	pwdbuf

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23222-TP.c
Method pqGetHomeDirectory(char *buf, int bufsize)

```
....
6050.        char        pwdbuf[BUFSIZ];
....
6054.        (void) pqGetpwuid(geteuid(), &pwdstr, pwdbuf,
sizeof(pwdbuf), &pwd);
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1141
Status	New

	Source	Destination
File	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c	php@@php-src-php-8.0.17-CVE-2020-1916-TP.c

Line	863	863
Object	ai	sizeof

Code Snippet
File Name php@@php-src-php-8.0.17-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
863.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1142
Status New

	Source	Destination
File	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c	php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Line	863	863
Object	ai	sizeof

Code Snippet
File Name php@@php-src-php-8.0.25-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
863.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1143
Status New

	Source	Destination
File	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c	php@@php-src-php-8.0.5-CVE-2020-1916-TP.c
Line	863	863
Object	ai	sizeof

Code Snippet
File Name php@@php-src-php-8.0.5-CVE-2020-1916-TP.c

Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
863.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1144
Status	New

	Source	Destination
File	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Line	855	855
Object	ai	sizeof

Code Snippet	
File Name	php@@php-src-php-8.1.27-CVE-2020-1916-TP.c
Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
855.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1145
Status	New

	Source	Destination
File	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Line	863	863
Object	ai	sizeof

Code Snippet	
File Name	php@@php-src-php-8.1.8-CVE-2020-1916-TP.c
Method	char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
863.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1146
Status	New

	Source	Destination
File	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c	php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Line	855	855
Object	ai	sizeof

Code Snippet
File Name php@@php-src-php-8.2.10-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
855.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1147
Status	New

	Source	Destination
File	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c	php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Line	855	855
Object	ai	sizeof

Code Snippet
File Name php@@php-src-php-8.2.18-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
855.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1148
Status	New

	Source	Destination
File	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c	php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Line	855	855
Object	ai	sizeof

Code Snippet
File Name php@@php-src-php-8.2.22-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
855.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1149
Status New

	Source	Destination
File	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c	php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Line	863	863
Object	ai	sizeof

Code Snippet
File Name php@@php-src-php-8.2.2-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
863.                    !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=1150
Status New

	Source	Destination
File	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c	php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Line	855	855

Object	ai	sizeof

Code Snippet
File Name php@@php-src-php-8.2.6-CVE-2020-1916-TP.c
Method char *php_crypt_blowfish_rn(const char *key, const char *setting,

```
....
855.                    !memcmp(ai, yi, sizeof(ai));
```

Use of Insufficiently Random Values

Query Path:
CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Insufficiently Random Values\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2878
Status	New

Method PostmasterRandom at line 5190 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c uses a weak method random to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5218	5218
Object	random	random

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterRandom(void)

```
....
5218.       return random();
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2879
Status	New

Method PostmasterRandom at line 5269 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c uses a weak method random to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5297	5297
Object	random	random

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method PostmasterRandom(void)

```
....
5297.       return random();
```

Use of Insufficiently Random Values\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2880
Status New

Method PostmasterMain at line 566 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c uses a weak method srandom to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	594	594
Object	srandom	srandom

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
594.        srandom((unsigned int) (MyProcPid ^ MyStartTime));
```

Use of Insufficiently Random Values\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2881
Status New

Method BackendRun at line 4281 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c uses a weak method srandom to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	4299	4299
Object	srandom	srandom

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method BackendRun(Port *port)

```
....
4299.       srandom((unsigned int) (MyProcPid ^ (usecs << 12) ^ secs));
```

Use of Insufficiently Random Values\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2882
Status New

Method PostmasterRandom at line 5190 of postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c uses a weak method srandom to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	5215	5215
Object	srandom	srandom

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterRandom(void)

```
....
5215.             srandom(random_seed);
```

Use of Insufficiently Random Values\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2883
Status New

Method PostmasterMain at line 578 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c uses a weak method srandom to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	606	606
Object	srandom	srandom

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
606.        srandom((unsigned int) (MyProcPid ^ MyStartTime));
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2884
Status	New

Method BackendRun at line 4317 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c uses a weak method srandom to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	4335	4335
Object	srandom	srandom

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method BackendRun(Port *port)

```
....
4335.       srandom((unsigned int) (MyProcPid ^ (usecs << 12) ^ secs));
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2885
Status	New

Method PostmasterRandom at line 5269 of postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c uses a weak method srandom to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	5294	5294
Object	srandom	srandom

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method PostmasterRandom(void)

```
....
5294.             srandom(random_seed);
```

Inconsistent Implementations

Query Path:
CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=393
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Line	665	665
Object	getopt	getopt

Code Snippet
File Name postgres@@postgres-REL9_6_18-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
665.         while ((opt = getopt(argc, argv,
"B:bc:C:D:d:EeFf:h:ijk:lN:nOo:Pp:r:S:sTt:W:-:")) != -1)
```

Inconsistent Implementations\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=394
Status New

	Source	Destination
File	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c	postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Line	684	684
Object	getopt	getopt

Code Snippet
File Name postgres@@postgres-REL9_6_20-CVE-2021-23214-TP.c
Method PostmasterMain(int argc, char *argv[])

```
....
684.        while ((opt = getopt(argc, argv,
"B:bc:C:D:d:EeFf:h:ijk:lN:nOo:Pp:r:S:sTt:W:-:")) != -1)
```

Inconsistent Implementations\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=395
Status New

	Source	Destination
File	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Line	2330	2330
Object	getopt_long	getopt_long

Code Snippet
File Name proftpd@@proftpd-v1.3.7-CVE-2023-51713-TP.c
Method int main(int argc, char *argv[], char **envp) {

```
....
2330.        getopt_long(argc, argv, cmdopts, opts, NULL)
```

Inconsistent Implementations\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=396
Status New

	Source	Destination
File	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c	proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c

Line	2475	2475
Object	getopt_long	getopt_long

Code Snippet
File Name proftpd@@proftpd-v1.3.8-CVE-2023-51713-TP.c
Method int main(int argc, char *argv[], char **envp) {

```
....
2475.        getopt_long(argc, argv, cmdopts, opts, NULL)
```

Information Exposure Through Comments

Query Path:
CPP\Cx\CPP Low Visibility\Information Exposure Through Comments Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)

Description

Information Exposure Through Comments\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2874
Status New

	Source	Destination
File	podofo@@podofo-0.10.0-rc1-CVE-2023-31555-FP.c	podofo@@podofo-0.10.0-rc1-CVE-2023-31555-FP.c
Line	1067	1067
Object	password:	password:

Code Snippet
File Name podofo@@podofo-0.10.0-rc1-CVE-2023-31555-FP.c
Method // Check password: 1) as user password, 2) as owner password

```
....
1067.      // Check password: 1) as user password, 2) as owner password
```

Information Exposure Through Comments\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2875
Status New

	Source	Destination

File	podofo@@podofo-0.10.0-rc1-CVE-2023-31555-FP.c	podofo@@podofo-0.10.0-rc1-CVE-2023-31555-FP.c
Line	1299	1299
Object	password:	password:

Code Snippet
File Name podofo@@podofo-0.10.0-rc1-CVE-2023-31555-FP.c
Method // Check password: 1) as user password, 2) as owner password

```
....
1299.       // Check password: 1) as user password, 2) as owner password
```

Information Exposure Through Comments\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2876
Status New

	Source	Destination
File	podofo@@podofo-0.10.0-rc1-CVE-2023-31568-TP.c	podofo@@podofo-0.10.0-rc1-CVE-2023-31568-TP.c
Line	1067	1067
Object	password:	password:

Code Snippet
File Name podofo@@podofo-0.10.0-rc1-CVE-2023-31568-TP.c
Method // Check password: 1) as user password, 2) as owner password

```
....
1067.       // Check password: 1) as user password, 2) as owner password
```

Information Exposure Through Comments\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=2877
Status New

	Source	Destination
File	podofo@@podofo-0.10.0-rc1-CVE-2023-31568-TP.c	podofo@@podofo-0.10.0-rc1-CVE-2023-31568-TP.c
Line	1299	1299
Object	password:	password:

Code Snippet	
File Name	podofo@@podofo-0.10.0-rc1-CVE-2023-31568-TP.c
Method	// Check password: 1) as user password, 2) as owner password

```
....
1299.       // Check password: 1) as user password, 2) as owner password
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=397
Status	New

The buffer allocated by <= in protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c at line 3019 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Line	3272	3272
Object	<=	<=

Code Snippet	
File Name	protobuf-c@@protobuf-c-v1.3.3-CVE-2022-48468-TP.c
Method	protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3272.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020058&projectid=20047&pathid=398
Status	New

The buffer allocated by <= in protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c at line 3026 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c	protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Line	3279	3279
Object	<=	<=

Code Snippet
File Name protobuf-c@@protobuf-c-v1.4.0-CVE-2022-48468-TP.c
Method protobuf_c_message_unpack(const ProtobufCMessageDescriptor *desc,

```
....
3279.       for (i_slab = 0; i_slab <= which_slab; i_slab++) {
```

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Off by One Error in Methods

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Short Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;

  void setPassword()
```

```
  {
      password = System.console().readLine("Enter your password: ");
   }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed

{
  private SealedObject password;

  void setPassword()

 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}

int main()

{

    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
```

```
	gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
	char* password = (char*) malloc(256);
	int i=0;
	char ch;
	ssize_t k;
	while(k = read(STDIN_FILENO, &ch, 1) > 0)
	{
		if (ch == '\n'){
			password[i]='\0';
			break;
		} else{
			password[i++]=ch;
			fflush(0);
		}
	}
	i=0;
	memset(password,'\0',256);
}

int main()

{

	printf("Please enter a password:\n");
	authfunc();
	somefunc();
	char ch;
	while(read(STDIN_FILENO, &ch, 1) > 0)
	{
		if (ch == '\n')
			break;
	}
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Stored Buffer Overflow fgets

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
```

```
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Insufficiently Protected Credentials

Risk

What might happen

An attacker could steal user credentials, enabling access to user accounts and confidential data.

Cause

How does it happen

User passwords are written to the database without being properly encrypted with a cryptographic hash. The application reads clear passwords straight from the database.

General Recommendations

How to avoid it

Store passwords using a cryptographic hash designed as a password protection scheme, such as:

- bcrypt
- scrypt
- PBKDF2 (with random salt) These need to be configured with an appropriately high work effort.

Source Code Examples

CSharp

Always use a secure password protection scheme to store passwords, such as bcrypt:

```
string hashed = BCrypt.HashPassword(password, BCrypt.GenerateSalt(12));
```

For password verification, use the matching function:

```
bool isValid = BCrypt.CheckPassword(candidate, hashed);
```

```
```

Java

Always use a secure password protection scheme to store passwords, such as bcrypt:

```
String hashed = BCrypt.hashpw(password, BCrypt.gensalt(12));
```

For password verification, use the matching function:

```
bool isValid = BCrypt.checkpw(candidate, hashed);
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
}

public static class decrementCounter extends Thread {
    public void run() {
       counter--;
    }
}
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
public static int counter = 0;
public static Object lock = new Object();

public static void start() throws InterruptedException {
       incrementCounter ic;
       decrementCounter dc;
       while(counter == 0) { // because of proper locking, this condition is never false
              counter = 0;
              ic = new incrementCounter();
              dc = new decrementCounter();
              ic.start();
              dc.start();
              ic.join();
              dc.join();
       }
       System.out.println(counter); // Never reached
}

public static class incrementCounter extends Thread {
    public void run() {
       synchronized (lock) {
              counter++;
       }
    }
}

public static class decrementCounter extends Thread {
    public void run() {
       synchronized (lock) {
              counter--;
       }
    }
}
```

Information Leak Through Comments

Weakness ID: 615 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

Time of Introduction

- Implementation

Demonstrative Examples

Example 1

The following comment, embedded in a JSP, will be displayed in the resulting HTML output.

(Bad Code)

Example Languages: **HTML and JSP**

```
<!-- FIXME: calling this with more than 30 args kills the JDBC server -->
```

Observed Examples

Reference	Description
CVE-2007-6197	Version numbers and internal hostnames leaked in HTML comments.
CVE-2007-4072	CMS places full pathname of server in HTML comment.
CVE-2009-2431	blog software leaks real username in HTML comment.

Potential Mitigations

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Variant	540	Information Leak Through Source Code	**Development Concepts (primary)699 Research Concepts (primary)1000**

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	Anonymous Tool Vendor (under NDA)		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal

	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Observed Examples, Taxonomy Mappings		

BACK TO TOP

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.
Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

```
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Resource Locking Problems

Category ID: 411 *(Category)* **Status:** Draft

Description

Description Summary

Weaknesses in this category are related to improper handling of locks that are used to control access to resources.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	412	Unrestricted Externally Accessible Lock	Development Concepts699
ParentOf	Weakness Base	413	Insufficient Resource Locking	**Development Concepts (primary)699**
ParentOf	Weakness Base	414	Missing Lock Check	**Development Concepts (primary)699**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Resource Locking problems

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025