vul_files_60 Scan Report

Project Name	vul_files_60
Scan Start	Wednesday, January 8, 2025 9:29:51 PM
Preset	Checkmarx Default
Scan Time	02h:13m:13s
Lines Of Code Scanned	298925
Files Scanned	363
Report Creation Time	Wednesday, January 8, 2025 11:48:19 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	4/1000 (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

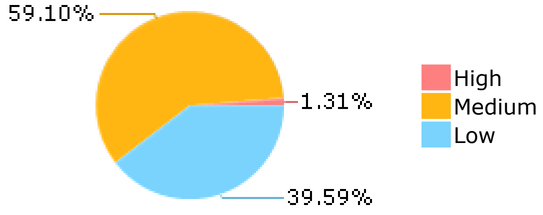
Results Limit

Results limit per query was set to 50

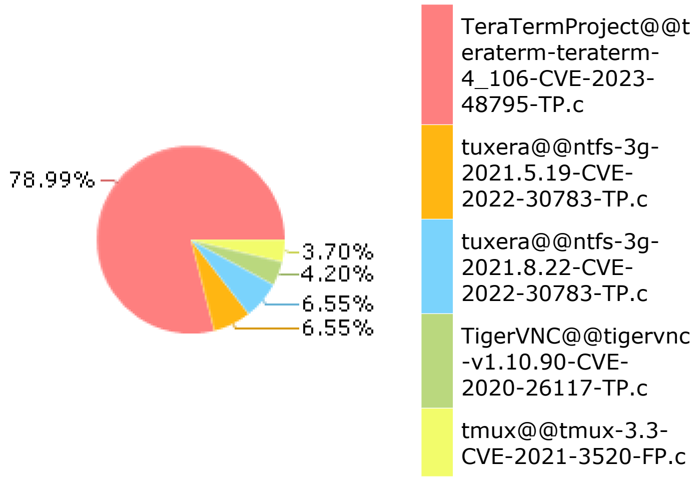
Selected Queries

Selected queries are listed in Result Summary

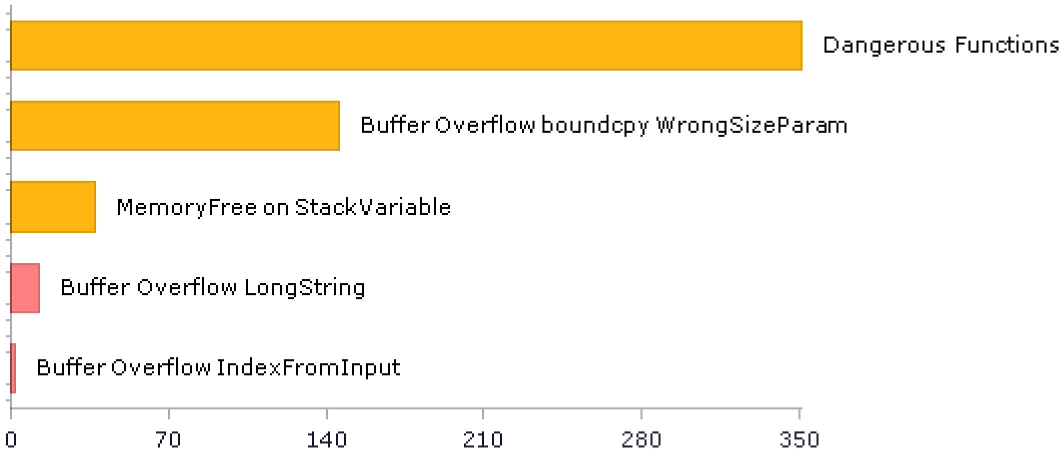
Result Summary



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	256	177
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	111	111
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	2	2
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	351	351
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	0	0
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	351	351
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	3	3
PCI DSS (3.2) - 6.5.2 - Buffer overflows	165	157
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.	20	20
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.	14	14
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.	91	91
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.	3	3
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.	7	7

***** 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)	125	125
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)	1	1
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)	2	2
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*****	137	58
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*****	27	19
SI-11 Error Handling (P2)*****	166	166
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	4	4

***** 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

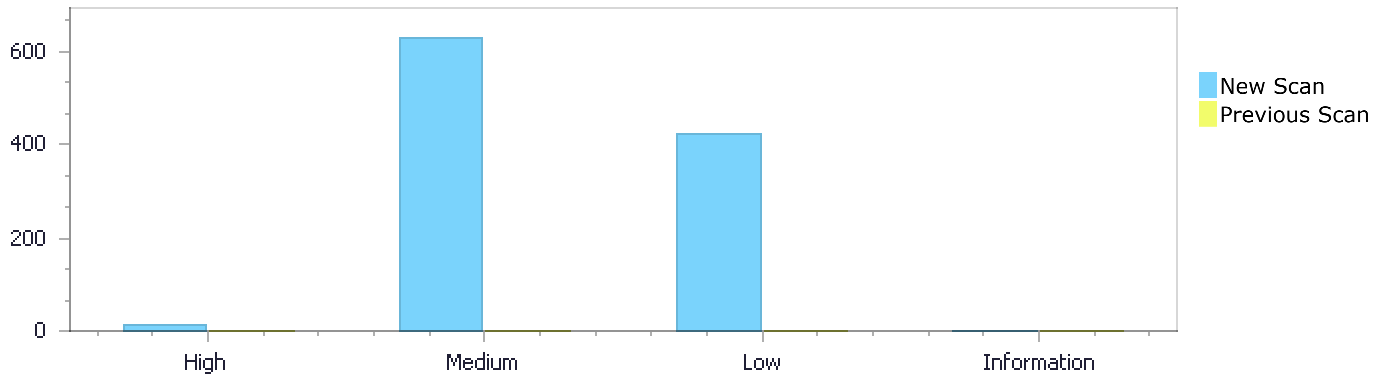
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	14	630	422	0	1,066
Recurrent Issues	0	0	0	0	0
Total	14	630	422	0	1,066

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	14	630	422	0	1,066
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	14	630	422	0	1,066

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow LongString	12	High
Buffer Overflow IndexFromInput	2	High
Dangerous Functions	351	Medium
Buffer Overflow boundcpy WrongSizeParam	146	Medium
MemoryFree on StackVariable	37	Medium

Wrong Size t Allocation	35	Medium
Memory Leak	28	Medium
Use of Zero Initialized Pointer	21	Medium
Integer Overflow	7	Medium
Use of Uninitialized Pointer	3	Medium
Double Free	1	Medium
Use of a One Way Hash without a Salt	1	Medium
Unchecked Return Value	166	Low
Improper Resource Access Authorization	91	Low
NULL Pointer Dereference	85	Low
TOCTOU	24	Low
Incorrect Permission Assignment For Critical Resources	20	Low
Exposure of System Data to Unauthorized Control Sphere	14	Low
Potential Precision Problem	8	Low
Use of Sizeof On a Pointer Type	6	Low
Potential Off by One Error in Loops	3	Low
Sizeof Pointer Argument	3	Low
Use of Insufficiently Random Values	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	243
tmux@@tmux-3.3-CVE-2021-3520-FP.c	22
ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c	18
ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c	18
ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c	18
ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c	18
ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c	18
tpm2-software@@tpm2-tss-4.1.0-rc0-CVE-2024-29040-TP.c	18
tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c	17
tpm2-software@@tpm2-tss-3.2.1-CVE-2024-29040-TP.c	17

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=1030073&projectid=30062&pathid=1
Status	New

The size of the buffer used by decode_string in sur, at line 295 of ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 295 of ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c
Line	317	422
Object	"Could not reserve memory block"	sur

Code Snippet

File Name	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c
Method	static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
317.          return SetError(ds, -1, "Could not reserve memory block");
....
422.                    sur[iSur] = (sur[iSur] << 4) + 10 + (JSUTF16)
(*inputOffset - 'A');
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=2
Status	New

The size of the buffer used by decode_string in sur, at line 295 of ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 295 of ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c
Line	317	413
Object	"Could not reserve memory block"	sur

Code Snippet

File Name	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c
Method	static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
317.          return SetError(ds, -1, "Could not reserve memory block");
....
413.                    sur[iSur] = (sur[iSur] << 4) + 10 + (JSUTF16)
(*inputOffset - 'a');
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=3
Status	New

The size of the buffer used by decode_string in sur, at line 295 of ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 295 of ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c
Line	317	404
Object	"Could not reserve memory block"	sur

Code Snippet

File Name	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c
Method	static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
317.          return SetError(ds, -1, "Could not reserve memory block");
....
404.                    sur[iSur] = (sur[iSur] << 4) + (JSUTF16)
(*inputOffset - '0');
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=4
Status	New

The size of the buffer used by decode_string in sur, at line 295 of ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 295 of ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c
Line	317	413
Object	"Could not reserve memory block"	sur

Code Snippet

File Name	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c
Method	static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
317.          return SetError(ds, -1, "Could not reserve memory block");
....
413.                   sur[iSur] = (sur[iSur] << 4) + 10 + (JSUTF16)
(*inputOffset - 'a');
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=5
Status	New

The size of the buffer used by decode_string in sur, at line 295 of ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 295 of ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c
Line	317	404
Object	"Could not reserve memory block"	sur

Code Snippet

File Name	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c

Method	static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
317.          return SetError(ds, -1, "Could not reserve memory block");
....
404.                      sur[iSur] = (sur[iSur] << 4) + (JSUTF16)
(*inputOffset - '0');
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=6
Status	New

The size of the buffer used by decode_string in sur, at line 295 of ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 295 of ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c
Line	317	422
Object	"Could not reserve memory block"	sur

Code Snippet	
File Name	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c
Method	static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
317.          return SetError(ds, -1, "Could not reserve memory block");
....
422.                      sur[iSur] = (sur[iSur] << 4) + 10 + (JSUTF16)
(*inputOffset - 'A');
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=7
Status	New

The size of the buffer used by decode_string in sur, at line 307 of ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 307 of ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination

File	ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c
Line	329	416
Object	"Could not reserve memory block"	sur

Code Snippet
File Name ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
329.            return SetError(ds, -1, "Could not reserve memory block");
....
416.                        sur[iSur] = (sur[iSur] << 4) + (JSUTF16)
(*inputOffset - '0');
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=8
Status	New

The size of the buffer used by decode_string in sur, at line 307 of ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 307 of ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c
Line	329	425
Object	"Could not reserve memory block"	sur

Code Snippet
File Name ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
329.            return SetError(ds, -1, "Could not reserve memory block");
....
425.                        sur[iSur] = (sur[iSur] << 4) + 10 + (JSUTF16)
(*inputOffset - 'a');
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30

	062&pathid=9
Status	New

The size of the buffer used by decode_string in sur, at line 307 of ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 307 of ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c
Line	329	434
Object	"Could not reserve memory block"	sur

Code Snippet
File Name ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
329.            return SetError(ds, -1, "Could not reserve memory block");
....
434.                       sur[iSur] = (sur[iSur] << 4) + 10 + (JSUTF16)
(*inputOffset - 'A');
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=10
Status	New

The size of the buffer used by decode_string in sur, at line 307 of ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 307 of ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c
Line	329	416
Object	"Could not reserve memory block"	sur

Code Snippet
File Name ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
329.         return SetError(ds, -1, "Could not reserve memory block");
....
416.                 sur[iSur] = (sur[iSur] << 4) + (JSUTF16)
(*inputOffset - '0');
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=11
Status	New

The size of the buffer used by decode_string in sur, at line 307 of ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 307 of ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c
Line	329	434
Object	"Could not reserve memory block"	sur

Code Snippet

File Name	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c
Method	static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
329.         return SetError(ds, -1, "Could not reserve memory block");
....
434.                 sur[iSur] = (sur[iSur] << 4) + 10 + (JSUTF16)
(*inputOffset - 'A');
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=12
Status	New

The size of the buffer used by decode_string in sur, at line 307 of ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_string passes to "Could not reserve memory block", at line 307 of ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c

Line	329	425
Object	"Could not reserve memory block"	sur

Code Snippet
File Name ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
329.          return SetError(ds, -1, "Could not reserve memory block");
....
425.                    sur[iSur] = (sur[iSur] << 4) + 10 + (JSUTF16)
(*inputOffset - 'a');
```

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=1030073&projectid=30062&pathid=13
Status	New

The size of the buffer used by parse_selection_data_from_selection_string in digest_list_count, at line 179 of tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_selection_data_from_selection_string passes to buffer, at line 179 of tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	237	236
Object	buffer	digest_list_count

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method static bool parse_selection_data_from_selection_string(FILE *pcr_input,

```
....
237.                      pcrs-
>pcr_values[digest_list_count].count].buffer,
....
236.                  read_count = fread(pcrs-
>pcr_values[digest_list_count].digests[
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=14
Status	New

The size of the buffer used by parse_selection_data_from_selection_string in digest_list_count, at line 179 of tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_selection_data_from_selection_string passes to buffer, at line 179 of tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	237	236
Object	buffer	digest_list_count

Code Snippet

File Name	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method	static bool parse_selection_data_from_selection_string(FILE *pcr_input,

```
....
237.                          pcrs-
>pcr_values[digest_list_count].buffer,
....
236.                      read_count = fread(pcrs-
>pcr_values[digest_list_count].digests[
```

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=1030073&projectid=30062&pathid=240
Status	New

The dangerous function, memcpy, was found in use at line 62 in tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Line	66	66
Object	memcpy	memcpy

Code Snippet
File Name tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Method TfLiteIntArray* TfLiteIntArrayCopy(const TfLiteIntArray* src) {

```
....
66.      memcpy(ret->data, src->data, src->size * sizeof(int));
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=241
Status	New

The dangerous function, memcpy, was found in use at line 191 in tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Line	203	203
Object	memcpy	memcpy

Code Snippet
File Name tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Method TfLiteStatus TfLiteTensorCopy(const TfLiteTensor* src, TfLiteTensor* dst) {

```
....
203.    memcpy(dst->data.raw, src->data.raw, src->bytes);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=242
Status	New

The dangerous function, memcpy, was found in use at line 64 in tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Line	68	68
Object	memcpy	memcpy

Code Snippet

File Name	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Method	TfLiteIntArray* TfLiteIntArrayCopy(const TfLiteIntArray* src) {

```
....
68.       memcpy(ret->data, src->data, src->size * sizeof(int));
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=243
Status	New

The dangerous function, memcpy, was found in use at line 193 in tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Line	205	205
Object	memcpy	memcpy

Code Snippet

File Name	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Method	TfLiteStatus TfLiteTensorCopy(const TfLiteTensor* src, TfLiteTensor* dst) {

```
....
205.     memcpy(dst->data.raw, src->data.raw, src->bytes);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=244
Status	New

The dangerous function, memcpy, was found in use at line 606 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	614	614
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void push_memdump(char *name, char *desc, char *data, int len)

```
....
614.        memcpy(dp, data, len);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=245
Status	New

The dangerous function, memcpy, was found in use at line 2384 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2396	2396
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void prep_pty(PTInstVar pvar)

```
....
2396.       memcpy(outmsg + 4, pvar->ts->TermType, len);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=246
Status	New

The dangerous function, memcpy, was found in use at line 2384 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2401	2401
Object	memcpy	memcpy

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static void prep_pty(PTInstVar pvar)

```
....
2401.       memcpy(outmsg + 4 + len + 16, ssh_ttymodes,
sizeof(ssh_ttymodes));
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=247
Status	New

The dangerous function, memcpy, was found in use at line 2567 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2629	2629
Object	memcpy	memcpy

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static BOOL handle_rsa_challenge(PTInstVar pvar)

```
....
2629.                   memcpy(session_buf + server_key_bytes +
host_key_bytes, pvar->crypt_state.server_cookie, 8);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=248
Status	New

The dangerous function, memcpy, was found in use at line 2567 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2640	2640
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_rsa_challenge(PTInstVar pvar)

```
....
2640.                   memcpy(outmsg, hash, 16);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=249
Status	New

The dangerous function, memcpy, was found in use at line 2652 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2683	2683
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void try_send_credentials(PTInstVar pvar)

```
....
2683.                        memcpy(outmsg + 4, cred->password, len);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=250
Status	New

The dangerous function, memcpy, was found in use at line 2652 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2700	2700
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void try_send_credentials(PTInstVar pvar)

```
....
2700.                           memcpy(outmsg + 4, cred-
>rhosts_client_user, len);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=251
Status	New

The dangerous function, memcpy, was found in use at line 2652 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2738	2738
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void try_send_credentials(PTInstVar pvar)

```
....
2738.                           memcpy(outmsg + 4, cred-
>rhosts_client_user, name_len);
```

Dangerous Functions\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=252
Status	New

The dangerous function, memcpy, was found in use at line 2652 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2783	2783
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void try_send_credentials(PTInstVar pvar)

```
....
2783.                          memcpy(outmsg + 2, pubkey, bn_bytes);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=253
Status	New

The dangerous function, memcpy, was found in use at line 2652 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2807	2807
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void try_send_credentials(PTInstVar pvar)

```
....
2807.                               memcpy(outmsg + 4, cred->password,
len);
```

Dangerous Functions\Path 15:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=254
Status	New

The dangerous function, memcpy, was found in use at line 2830 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2845	2845
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void try_send_user_name(PTInstVar pvar)

```
....
2845.                     memcpy(outmsg + 4, username, len);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=255
Status	New

The dangerous function, memcpy, was found in use at line 2857 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2875	2875
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void send_session_key(PTInstVar pvar)

```
....
2875.                memcpy(outmsg + 1, CRYPT_get_server_cookie(pvar), 8);
       /* antispoofing cookie */
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=256
Status	New

The dangerous function, memcpy, was found in use at line 2957 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2966	2966
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH_notify_disconnecting(PTInstVar pvar, char *reason)

```
....
2966.                         memcpy(outmsg + 4, reason, len);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=257
Status	New

The dangerous function, memcpy, was found in use at line 2957 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2990	2990
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH_notify_disconnecting(PTInstVar pvar, char *reason)

```
....
2990.                   memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=258
Status	New

The dangerous function, memcpy, was found in use at line 3026 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3085	3085
Object	memcpy	memcpy

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH_notify_win_size(PTInstVar pvar, int cols, int rows)

```
....
3085.            memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=259
Status	New

The dangerous function, memcpy, was found in use at line 3101 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3136	3136
Object	memcpy	memcpy

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method int SSH_notify_break_signal(PTInstVar pvar)

```
....
3136.                memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=260
Status	New

The dangerous function, memcpy, was found in use at line 3210 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3262	3262
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_send(PTInstVar pvar, unsigned char const *buf, unsigned int buflen)

```
....
3262.                             memcpy(outmsg + 4, buf, len);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=261
Status	New

The dangerous function, memcpy, was found in use at line 3283 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3292	3292
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method int SSH_extract_payload(PTInstVar pvar, unsigned char *dest, int len)

```
....
3292.            memcpy(dest,
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=262
Status	New

The dangerous function, memcpy, was found in use at line 3526 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3574	3574
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3574.            memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=263
Status	New

The dangerous function, memcpy, was found in use at line 3592 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3633	3633
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_channel_send(PTInstVar pvar, int channel_num,

```
....
3633.                      memcpy(outmsg + 8, buf, len);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=264
Status	New

The dangerous function, memcpy, was found in use at line 3646 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3674	3674
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_fail_channel_open(PTInstVar pvar, uint32 remote_channel_num)

```
....
3674.                memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=265
Status	New

The dangerous function, memcpy, was found in use at line 3682 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3703	3703
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH2_confirm_channel_open(PTInstVar pvar, Channel_t *c)

```
....
3703.		memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=266
Status	New

The dangerous function, memcpy, was found in use at line 3749 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3778	3778
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH2_channel_input_eof(PTInstVar pvar, Channel_t *c)

```
....
3778.		memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=267
Status	New

The dangerous function, memcpy, was found in use at line 3806 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3820	3820

Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH_request_forwarding(PTInstVar pvar, char *bind_address, int from_server_port,

```
....
3820.               memcpy(outmsg + 8, to_local_host, host_len);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=268
Status	New

The dangerous function, memcpy, was found in use at line 3806 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3856	3856
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH_request_forwarding(PTInstVar pvar, char *bind_address, int from_server_port,

```
....
3856.               memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=269
Status	New

The dangerous function, memcpy, was found in use at line 3866 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3889	3889
Object	memcpy	memcpy

Code Snippet
File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH_cancel_request_forwarding(PTInstVar pvar, char *bind_address, int from_server_port, int reply)

```
....
3889.            memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=270
Status	New

The dangerous function, memcpy, was found in use at line 3897 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3912	3912
Object	memcpy	memcpy

Code Snippet
File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH_request_X11_forwarding(PTInstVar pvar,

```
....
3912.            memcpy(outmsg + 4, auth_protocol, protocol_len);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=271
Status	New

The dangerous function, memcpy, was found in use at line 3897 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3975	3975
Object	memcpy	memcpy

Code Snippet
File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH_request_X11_forwarding(PTInstVar pvar,

```
....
3975.                memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=272
Status	New

The dangerous function, memcpy, was found in use at line 3988 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4008	4008
Object	memcpy	memcpy

Code Snippet
File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH_open_channel(PTInstVar pvar, uint32 local_channel_num,

```
....
4008.                memcpy(outmsg + 8, to_remote_host, host_len);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=273
Status	New

The dangerous function, memcpy, was found in use at line 3988 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4011	4011
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_open_channel(PTInstVar pvar, uint32 local_channel_num,

```
....
4011.            memcpy(outmsg + 16 + host_len, originator,
originator_len);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=274
Status	New

The dangerous function, memcpy, was found in use at line 3988 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4021	4021
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_open_channel(PTInstVar pvar, uint32 local_channel_num,

```
....
4021.                  memcpy(outmsg + 8, to_remote_host, host_len);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=275
Status	New

The dangerous function, memcpy, was found in use at line 3988 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4077	4077
Object	memcpy	memcpy

Code Snippet
File Name   TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method   void SSH_open_channel(PTInstVar pvar, uint32 local_channel_num,

```
....
4077.                        memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=276
Status	New

The dangerous function, memcpy, was found in use at line 4103 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4233	4233
Object	memcpy	memcpy

Code Snippet
File Name   TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method   int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4233.        memcpy(outmsg, buffer_ptr (msg), len);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=277

Status	New

The dangerous function, memcpy, was found in use at line 4268 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4306	4306
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method int SSH_sftp_transaction(PTInstVar pvar)

```
....
4306.       memcpy(outmsg, buffer_ptr (msg), len);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=278
Status	New

The dangerous function, memcpy, was found in use at line 4380 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4448	4448
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH2_send_kexinit(PTInstVar pvar)

```
....
4448.       memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30

	062&pathid=279
Status	New

The dangerous function, memcpy, was found in use at line 5008 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5050	5050
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void SSH2_dh_kex_init(PTInstVar pvar)

```
....
5050.        memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=280
Status	New

The dangerous function, memcpy, was found in use at line 5086 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5143	5143
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void SSH2_dh_gex_kex_init(PTInstVar pvar)

```
....
5143.        memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 42:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=281
Status	New

The dangerous function, memcpy, was found in use at line 5180 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5277	5277
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static BOOL handle_SSH2_dh_gex_group(PTInstVar pvar)

```
....
5277.        memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=282
Status	New

The dangerous function, memcpy, was found in use at line 5319 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5357	5357
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void SSH2_ecdh_kex_init(PTInstVar pvar)

```
....
5357.        memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=283
Status	New

The dangerous function, memcpy, was found in use at line 5399 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5416	5416
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL ssh2_kex_finish(PTInstVar pvar, char *hash, int hashlen, BIGNUM *share_key, Key *hostkey, char *signature, int siglen)

```
....
5416.                   memcpy(pvar->session_id, hash, pvar-
>session_id_len);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=284
Status	New

The dangerous function, memcpy, was found in use at line 5487 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5492	5492
Object	memcpy	memcpy

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL store_contents_for_known_hosts(PTInstVar pvar, enum ssh_kex_known_hosts kex_type, UINT_PTR offset)

```
....
5492.        memcpy(pvar->contents_after_known_hosts.payload, pvar-
>ssh_state.payload, pvar->ssh_state.payloadlen);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=285
Status	New

The dangerous function, memcpy, was found in use at line 6472 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	6506	6506
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	BOOL do_SSH2_userauth(PTInstVar pvar)

```
....
6506.        memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=286
Status	New

The dangerous function, memcpy, was found in use at line 6552 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	6707	6707
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	BOOL do_SSH2_authrequest(PTInstVar pvar)

```
....
6707.         memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=287
Status	New

The dangerous function, memcpy, was found in use at line 6738 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	6767	6767
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static LRESULT CALLBACK ssh_heartbeat_dlg_proc(HWND hWnd, UINT msg, WPARAM wp, LPARAM lp)

```
....
6767.                         memcpy(outmsg, buffer_ptr(msg), len);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=288
Status	New

The dangerous function, memcpy, was found in use at line 6878 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	6939	6939
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static BOOL handle_SSH2_userauth_success(PTInstVar pvar)

```
....
6939.                memcpy(outmsg, buffer_ptr (msg), len);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=289
Status	New

The dangerous function, memcpy, was found in use at line 7257 in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	7368	7368
Object	memcpy	memcpy

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	BOOL handle_SSH2_userauth_inforeq(PTInstVar pvar)

```
....
7368.        memcpy(outmsg, buffer_ptr(msg), len);
```

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=1030073&projectid=30062&pathid=15
Status	New

The size of the buffer used by prep_pty in ssh_ttymodes, at line 2384 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that prep_pty passes to ssh_ttymodes, at line 2384 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, to overwrite the target buffer.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2401	2401
Object	ssh_ttymodes	ssh_ttymodes

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void prep_pty(PTInstVar pvar)

```
....
2401.        memcpy(outmsg + 4 + len + 16, ssh_ttymodes,
sizeof(ssh_ttymodes));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=16
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF16, at line 263 of ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF16, at line 263 of ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Line	312	312
Object	JSUTF16	JSUTF16

Code Snippet
File Name ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Method static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
312.          memcpy(&in16, io, sizeof(JSUTF16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30

	062&pathid=17
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF16, at line 263 of ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF16, at line 263 of ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Line	345	345
Object	JSUTF16	JSUTF16

Code Snippet

File Name	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Method	static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
345.            memcpy(&in16, io, sizeof(JSUTF16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=18
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUINT8, at line 263 of ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUINT8, at line 263 of ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Line	346	346
Object	JSUINT8	JSUINT8

Code Snippet

File Name	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Method	static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
346.            memcpy(&in8, io + 2, sizeof(JSUINT8));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=19
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF32, at line 263 of ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF32, at line 263 of ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Line	378	378
Object	JSUTF32	JSUTF32

Code Snippet

File Name	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Method	static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
378.          memcpy(&in, io, sizeof(JSUTF32));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=20
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF16, at line 263 of ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF16, at line 263 of ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Line	312	312
Object	JSUTF16	JSUTF16

Code Snippet

File Name	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Method	static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
312.          memcpy(&in16, io, sizeof(JSUTF16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=21
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF16, at line 263 of ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF16, at line 263 of ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Line	345	345
Object	JSUTF16	JSUTF16

Code Snippet	
File Name	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Method	static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
345.            memcpy(&in16, io, sizeof(JSUTF16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=22
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUINT8, at line 263 of ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUINT8, at line 263 of ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Line	346	346
Object	JSUINT8	JSUINT8

Code Snippet	
File Name	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Method	static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
346.          memcpy(&in8, io + 2, sizeof(JSUINT8));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=23
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF32, at line 263 of ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF32, at line 263 of ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Line	378	378
Object	JSUTF32	JSUTF32

Code Snippet

File Name ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c

Method static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
378.          memcpy(&in, io, sizeof(JSUTF32));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=24
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF16, at line 263 of ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF16, at line 263 of ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Line	312	312
Object	JSUTF16	JSUTF16

Code Snippet

File Name	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Method	static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
312.          memcpy(&in16, io, sizeof(JSUTF16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=25
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF16, at line 263 of ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF16, at line 263 of ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Line	345	345
Object	JSUTF16	JSUTF16

Code Snippet

File Name	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Method	static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
345.          memcpy(&in16, io, sizeof(JSUTF16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=26
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUINT8, at line 263 of ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUINT8, at line 263 of ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Line	346	346

Object	JSUINT8	JSUINT8

Code Snippet
File Name ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Method static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
346.            memcpy(&in8, io + 2, sizeof(JSUINT8));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=27
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF32, at line 263 of ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF32, at line 263 of ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Line	378	378
Object	JSUTF32	JSUTF32

Code Snippet
File Name ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Method static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
378.            memcpy(&in, io, sizeof(JSUTF32));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=28
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF16, at line 262 of ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF16, at line 262 of ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination

File	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Line	311	311
Object	JSUTF16	JSUTF16

Code Snippet
File Name ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Method static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
311.          memcpy(&in16, io, sizeof(JSUTF16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=29
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF16, at line 262 of ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF16, at line 262 of ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Line	344	344
Object	JSUTF16	JSUTF16

Code Snippet
File Name ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Method static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
344.          memcpy(&in16, io, sizeof(JSUTF16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=30
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUINT8, at line 262 of ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer.

This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUINT8, at line 262 of ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Line	345	345
Object	JSUINT8	JSUINT8

Code Snippet
File Name ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Method static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
345.          memcpy(&in8, io + 2, sizeof(JSUINT8));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=31
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF32, at line 262 of ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF32, at line 262 of ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Line	377	377
Object	JSUTF32	JSUTF32

Code Snippet
File Name ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Method static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
377.          memcpy(&in, io, sizeof(JSUTF32));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=32
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF16, at line 262 of ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF16, at line 262 of ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Line	311	311
Object	JSUTF16	JSUTF16

Code Snippet
File Name ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Method static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
311.          memcpy(&in16, io, sizeof(JSUTF16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=33
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF16, at line 262 of ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF16, at line 262 of ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Line	344	344
Object	JSUTF16	JSUTF16

Code Snippet
File Name ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Method static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
344.          memcpy(&in16, io, sizeof(JSUTF16));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=34
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUINT8, at line 262 of ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUINT8, at line 262 of ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Line	345	345
Object	JSUINT8	JSUINT8

Code Snippet

File Name	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Method	static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
345.          memcpy(&in8, io + 2, sizeof(JSUINT8));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=35
Status	New

The size of the buffer used by Buffer_EscapeStringValidated in JSUTF32, at line 262 of ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Buffer_EscapeStringValidated passes to JSUTF32, at line 262 of ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c, to overwrite the target buffer.

	Source	Destination
File	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Line	377	377
Object	JSUTF32	JSUTF32

Code Snippet

File Name	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Method	static int Buffer_EscapeStringValidated (JSOBJ obj, JSONObjectEncoder *enc, const char *io, const char *end)

```
....
377.          memcpy(&in, io, sizeof(JSUTF32));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=36
Status	New

The size of the buffer used by *ssh2_channel_new in Channel_t, at line 188 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ssh2_channel_new passes to Channel_t, at line 188 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, to overwrite the target buffer.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	207	207
Object	Channel_t	Channel_t

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static Channel_t *ssh2_channel_new(unsigned int window, unsigned int maxpack,

```
....
207.        memset(c, 0, sizeof(Channel_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=37
Status	New

The size of the buffer used by ssh2_channel_delete in Channel_t, at line 313 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh2_channel_delete passes to Channel_t, at line 313 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, to overwrite the target buffer.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	369	369
Object	Channel_t	Channel_t

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static void ssh2_channel_delete(Channel_t *c)

```
....
369.        memset(c, 0, sizeof(Channel_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=38
Status	New

The size of the buffer used by SSH_init in ->, at line 2905 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SSH_init passes to ->, at line 2905 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, to overwrite the target buffer.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2929	2929
Object	->	->

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH_init(PTInstVar pvar)

```
....
2929.       memset(pvar->ssh2_keys, 0, sizeof(pvar->ssh2_keys));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=39
Status	New

The size of the buffer used by SSH_end in ->, at line 3403 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SSH_end passes to ->, at line 3403 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, to overwrite the target buffer.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3463	3463
Object	->	->

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH_end(PTInstVar pvar)

```
....
3463.              memset(pvar->server_version_string, 0, sizeof(pvar-
>server_version_string));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=40
Status	New

The size of the buffer used by SSH_end in ->, at line 3403 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SSH_end passes to ->, at line 3403 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, to overwrite the target buffer.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3464	3464
Object	->	->

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_end(PTInstVar pvar)

```
....
3464.              memset(pvar->client_version_string, 0, sizeof(pvar-
>client_version_string));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=41
Status	New

The size of the buffer used by parse_selection_data_from_selection_string in tpm2_pcrs, at line 179 of tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_selection_data_from_selection_string passes to tpm2_pcrs, at line 179 of tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	204	204
Object	tpm2_pcrs	tpm2_pcrs

Code Snippet	
File Name	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method	static bool parse_selection_data_from_selection_string(FILE *pcr_input,

```
....
204.        memset(pcrs, 0, sizeof(tpm2_pcrs));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=42
Status	New

The size of the buffer used by parse_selection_data_from_selection_string in tpm2_pcrs, at line 179 of tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_selection_data_from_selection_string passes to tpm2_pcrs, at line 179 of tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	204	204
Object	tpm2_pcrs	tpm2_pcrs

Code Snippet	
File Name	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method	static bool parse_selection_data_from_selection_string(FILE *pcr_input,

```
....
204.        memset(pcrs, 0, sizeof(tpm2_pcrs));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=43
Status	New

The size of the buffer used by ifapi_json_TPMS_PCR_SELECT_deserialize in TPMS_PCR_SELECT, at line 327 of tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMS_PCR_SELECT_deserialize passes to TPMS_PCR_SELECT, at line 327 of tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c

Line	331	331
Object	TPMS_PCR_SELECT	TPMS_PCR_SELECT

Code Snippet
File Name tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Method ifapi_json_TPMS_PCR_SELECT_deserialize(json_object *jso, TPMS_PCR_SELECT *out)

```
....
331.      memset(out, 0, sizeof(TPMS_PCR_SELECT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=44
Status	New

The size of the buffer used by ifapi_json_TPMS_PCR_SELECTION_deserialize in TPMS_PCR_SELECTION, at line 344 of tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMS_PCR_SELECTION_deserialize passes to TPMS_PCR_SELECTION, at line 344 of tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Line	351	351
Object	TPMS_PCR_SELECTION	TPMS_PCR_SELECTION

Code Snippet
File Name tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Method ifapi_json_TPMS_PCR_SELECTION_deserialize(json_object *jso,

```
....
351.      memset(out, 0, sizeof(TPMS_PCR_SELECTION));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=45
Status	New

The size of the buffer used by ifapi_json_TPMA_OBJECT_deserialize in TPMA_OBJECT, at line 987 of tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_OBJECT_deserialize passes to TPMA_OBJECT, at line 987 of tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Line	1009	1009
Object	TPMA_OBJECT	TPMA_OBJECT

Code Snippet
File Name tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Method ifapi_json_TPMA_OBJECT_deserialize(json_object *jso, TPMA_OBJECT *out)

```
....
1009.       memset(out, 0, sizeof(TPMA_OBJECT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=46
Status	New

The size of the buffer used by ifapi_json_TPMA_LOCALITY_deserialize in TPMA_LOCALITY, at line 1077 of tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_LOCALITY_deserialize passes to TPMA_LOCALITY, at line 1077 of tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Line	1093	1093
Object	TPMA_LOCALITY	TPMA_LOCALITY

Code Snippet
File Name tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Method ifapi_json_TPMA_LOCALITY_deserialize(json_object *jso, TPMA_LOCALITY *out)

```
....
1093.       memset(out, 0, sizeof(TPMA_LOCALITY));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=47
Status	New

The size of the buffer used by ifapi_json_TPMA_NV_deserialize in TPMA_NV, at line 3900 of tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer.

This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_NV_deserialize passes to TPMA_NV, at line 3900 of tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Line	3938	3938
Object	TPMA_NV	TPMA_NV

Code Snippet

File Name	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Method	ifapi_json_TPMA_NV_deserialize(json_object *jso, TPMA_NV *out)

```
....
3938.       memset(out, 0, sizeof(TPMA_NV));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=48
Status	New

The size of the buffer used by ifapi_json_TPMS_PCR_SELECT_deserialize in TPMS_PCR_SELECT, at line 333 of tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMS_PCR_SELECT_deserialize passes to TPMS_PCR_SELECT, at line 333 of tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Line	337	337
Object	TPMS_PCR_SELECT	TPMS_PCR_SELECT

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Method	ifapi_json_TPMS_PCR_SELECT_deserialize(json_object *jso, TPMS_PCR_SELECT *out)

```
....
337.       memset(out, 0, sizeof(TPMS_PCR_SELECT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=49

Status	New

The size of the buffer used by ifapi_json_TPMS_PCR_SELECTION_deserialize in TPMS_PCR_SELECTION, at line 350 of tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMS_PCR_SELECTION_deserialize passes to TPMS_PCR_SELECTION, at line 350 of tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Line	357	357
Object	TPMS_PCR_SELECTION	TPMS_PCR_SELECTION

Code Snippet
File Name tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Method ifapi_json_TPMS_PCR_SELECTION_deserialize(json_object *jso,

```
....
357.        memset(out, 0, sizeof(TPMS_PCR_SELECTION));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=50
Status	New

The size of the buffer used by ifapi_json_TPMA_OBJECT_deserialize in TPMA_OBJECT, at line 993 of tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_OBJECT_deserialize passes to TPMA_OBJECT, at line 993 of tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Line	1015	1015
Object	TPMA_OBJECT	TPMA_OBJECT

Code Snippet
File Name tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Method ifapi_json_TPMA_OBJECT_deserialize(json_object *jso, TPMA_OBJECT *out)

```
....
1015.        memset(out, 0, sizeof(TPMA_OBJECT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=51
Status	New

The size of the buffer used by ifapi_json_TPMA_LOCALITY_deserialize in TPMA_LOCALITY, at line 1083 of tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_LOCALITY_deserialize passes to TPMA_LOCALITY, at line 1083 of tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Line	1099	1099
Object	TPMA_LOCALITY	TPMA_LOCALITY

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Method	ifapi_json_TPMA_LOCALITY_deserialize(json_object *jso, TPMA_LOCALITY *out)

```
....
1099.       memset(out, 0, sizeof(TPMA_LOCALITY));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=52
Status	New

The size of the buffer used by ifapi_json_TPMA_NV_deserialize in TPMA_NV, at line 3863 of tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_NV_deserialize passes to TPMA_NV, at line 3863 of tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Line	3901	3901
Object	TPMA_NV	TPMA_NV

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Method	ifapi_json_TPMA_NV_deserialize(json_object *jso, TPMA_NV *out)

```
....
3901.       memset(out, 0, sizeof(TPMA_NV));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=53
Status	New

The size of the buffer used by ifapi_json_TPMS_PCR_SELECT_deserialize in TPMS_PCR_SELECT, at line 334 of tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMS_PCR_SELECT_deserialize passes to TPMS_PCR_SELECT, at line 334 of tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Line	338	338
Object	TPMS_PCR_SELECT	TPMS_PCR_SELECT

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Method	ifapi_json_TPMS_PCR_SELECT_deserialize(json_object *jso, TPMS_PCR_SELECT *out)

```
....
338.        memset(out, 0, sizeof(TPMS_PCR_SELECT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=54
Status	New

The size of the buffer used by ifapi_json_TPMS_PCR_SELECTION_deserialize in TPMS_PCR_SELECTION, at line 358 of tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMS_PCR_SELECTION_deserialize passes to TPMS_PCR_SELECTION, at line 358 of tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Line	365	365
Object	TPMS_PCR_SELECTION	TPMS_PCR_SELECTION

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Method	ifapi_json_TPMS_PCR_SELECTION_deserialize(json_object *jso,

```
....
365.        memset(out, 0, sizeof(TPMS_PCR_SELECTION));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=55
Status	New

The size of the buffer used by ifapi_json_TPMA_OBJECT_deserialize in TPMA_OBJECT, at line 1003 of tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_OBJECT_deserialize passes to TPMA_OBJECT, at line 1003 of tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Line	1025	1025
Object	TPMA_OBJECT	TPMA_OBJECT

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Method	ifapi_json_TPMA_OBJECT_deserialize(json_object *jso, TPMA_OBJECT *out)

```
....
1025.       memset(out, 0, sizeof(TPMA_OBJECT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=56
Status	New

The size of the buffer used by ifapi_json_TPMA_LOCALITY_deserialize in TPMA_LOCALITY, at line 1093 of tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_LOCALITY_deserialize passes to TPMA_LOCALITY, at line 1093 of tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Line	1109	1109
Object	TPMA_LOCALITY	TPMA_LOCALITY

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Method	ifapi_json_TPMA_LOCALITY_deserialize(json_object *jso, TPMA_LOCALITY *out)

```
....
1109.       memset(out, 0, sizeof(TPMA_LOCALITY));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=57
Status	New

The size of the buffer used by ifapi_json_TPMA_NV_deserialize in TPMA_NV, at line 4207 of tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_NV_deserialize passes to TPMA_NV, at line 4207 of tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Line	4245	4245
Object	TPMA_NV	TPMA_NV

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Method	ifapi_json_TPMA_NV_deserialize(json_object *jso, TPMA_NV *out)

```
....
4245.       memset(out, 0, sizeof(TPMA_NV));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=58
Status	New

The size of the buffer used by ifapi_json_TPMS_PCR_SELECT_deserialize in TPMS_PCR_SELECT, at line 378 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMS_PCR_SELECT_deserialize passes to TPMS_PCR_SELECT, at line 378 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c

Line	382	382
Object	TPMS_PCR_SELECT	TPMS_PCR_SELECT

Code Snippet
File Name tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Method ifapi_json_TPMS_PCR_SELECT_deserialize(json_object *jso, TPMS_PCR_SELECT *out)

```
....
382.       memset(out, 0, sizeof(TPMS_PCR_SELECT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=59
Status	New

The size of the buffer used by ifapi_json_TPMS_PCR_SELECTION_deserialize in TPMS_PCR_SELECTION, at line 402 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMS_PCR_SELECTION_deserialize passes to TPMS_PCR_SELECTION, at line 402 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Line	409	409
Object	TPMS_PCR_SELECTION	TPMS_PCR_SELECTION

Code Snippet
File Name tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Method ifapi_json_TPMS_PCR_SELECTION_deserialize(json_object *jso,

```
....
409.       memset(out, 0, sizeof(TPMS_PCR_SELECTION));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=60
Status	New

The size of the buffer used by ifapi_json_TPMS_TAGGED_POLICY_deserialize in TPMS_TAGGED_POLICY, at line 442 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMS_TAGGED_POLICY_deserialize passes to TPMS_TAGGED_POLICY, at line 442 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Line	450	450
Object	TPMS_TAGGED_POLICY	TPMS_TAGGED_POLICY

Code Snippet
File Name tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Method ifapi_json_TPMS_TAGGED_POLICY_deserialize(json_object *jso,

```
....
450.       memset(out, 0, sizeof(TPMS_TAGGED_POLICY));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=61
Status	New

The size of the buffer used by ifapi_json_TPMS_ACT_DATA_deserialize in TPMS_ACT_DATA, at line 487 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMS_ACT_DATA_deserialize passes to TPMS_ACT_DATA, at line 487 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Line	495	495
Object	TPMS_ACT_DATA	TPMS_ACT_DATA

Code Snippet
File Name tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Method ifapi_json_TPMS_ACT_DATA_deserialize(json_object *jso,

```
....
495.       memset(out, 0, sizeof(TPMS_ACT_DATA));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=62
Status	New

The size of the buffer used by ifapi_json_TPMA_OBJECT_deserialize in TPMA_OBJECT, at line 1143 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_OBJECT_deserialize passes to TPMA_OBJECT, at line 1143 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Line	1165	1165
Object	TPMA_OBJECT	TPMA_OBJECT

Code Snippet
File Name tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Method ifapi_json_TPMA_OBJECT_deserialize(json_object *jso, TPMA_OBJECT *out)

```
....
1165.       memset(out, 0, sizeof(TPMA_OBJECT));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=63
Status	New

The size of the buffer used by ifapi_json_TPMA_LOCALITY_deserialize in TPMA_LOCALITY, at line 1233 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_LOCALITY_deserialize passes to TPMA_LOCALITY, at line 1233 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Line	1249	1249
Object	TPMA_LOCALITY	TPMA_LOCALITY

Code Snippet
File Name tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Method ifapi_json_TPMA_LOCALITY_deserialize(json_object *jso, TPMA_LOCALITY *out)

```
....
1249.       memset(out, 0, sizeof(TPMA_LOCALITY));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=64
Status	New

The size of the buffer used by ifapi_json_TPMA_ACT_deserialize in TPMA_ACT, at line 1332 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ifapi_json_TPMA_ACT_deserialize passes to TPMA_ACT, at line 1332 of tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c, to overwrite the target buffer.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Line	1345	1345
Object	TPMA_ACT	TPMA_ACT

Code Snippet
File Name tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Method ifapi_json_TPMA_ACT_deserialize(json_object *jso, TPMA_ACT *out) {

```
....
1345.      memset(out, 0, sizeof(TPMA_ACT));
```

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=1030073&projectid=30062&pathid=161
Status	New

Calling free() (line 105) on a variable that was not dynamically allocated (line 105) in file tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c may result with a crash.

	Source	Destination
File	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Line	117	117
Object	q_params	q_params

Code Snippet
File Name tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Method void TfLiteQuantizationFree(TfLiteQuantization* quantization) {

```
....
117.      free(q_params);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=162
Status	New

Calling free() (line 107) on a variable that was not dynamically allocated (line 107) in file tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c may result with a crash.

	Source	Destination
File	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Line	119	119
Object	q_params	q_params

Code Snippet

File Name tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c

Method void TfLiteQuantizationFree(TfLiteQuantization* quantization) {

```
....
119.        free(q_params);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=163
Status	New

Calling free() (line 276) on a variable that was not dynamically allocated (line 276) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	298	298
Object	ch	ch

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static void ssh2_channel_retry_send_bufchain(PTInstVar pvar, Channel_t *c)

```
....
298.                free(ch);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=164
Status	New

Calling free() (line 313) on a variable that was not dynamically allocated (line 313) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	324	324
Object	ptr	ptr

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void ssh2_channel_delete(Channel_t *c)

```
....
324.                    free(ptr);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=165
Status	New

Calling free() (line 1384) on a variable that was not dynamically allocated (line 1384) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1414	1414
Object	cur_item	cur_item

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void deque_handlers(PTInstVar pvar, int message)

```
....
1414.                   free(cur_item);
```

MemoryFree on StackVariable\Path 6:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=166
Status	New

Calling free() (line 2567) on a variable that was not dynamically allocated (line 2567) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2641	2641
Object	hash	hash

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static BOOL handle_rsa_challenge(PTInstVar pvar)

```
....
2641.                   free(hash);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=167
Status	New

Calling free() (line 3403) on a variable that was not dynamically allocated (line 3403) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3419	3419
Object	cur_item	cur_item

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH_end(PTInstVar pvar)

```
....
3419.                        free(cur_item);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30

	062&pathid=168
Status	New

Calling free() (line 6519) on a variable that was not dynamically allocated (line 6519) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	6530	6530
Object	svc	svc

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_service_accept(PTInstVar pvar)

```
....
6530.        free(svc);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=169
Status	New

Calling free() (line 6552) on a variable that was not dynamically allocated (line 6552) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	6663	6663
Object	signature	signature

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL do_SSH2_authrequest(PTInstVar pvar)

```
....
6663.              free(signature);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=170

Status	New

Calling free() (line 7118) on a variable that was not dynamically allocated (line 7118) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	7191	7191
Object	msgA	msgA

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_userauth_banner(PTInstVar pvar)

```
....
7191.                               free(msgA);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=171
Status	New

Calling free() (line 7118) on a variable that was not dynamically allocated (line 7118) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	7198	7198
Object	msgA	msgA

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_userauth_banner(PTInstVar pvar)

```
....
7198.                               free(msgA);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=172
Status	New

Calling free() (line 7257) on a variable that was not dynamically allocated (line 7257) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	7303	7303
Object	name	name

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL handle_SSH2_userauth_inforeq(PTInstVar pvar)

```
....
7303.        free(name);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=173
Status	New

Calling free() (line 7257) on a variable that was not dynamically allocated (line 7257) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	7304	7304
Object	inst	inst

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL handle_SSH2_userauth_inforeq(PTInstVar pvar)

```
....
7304.        free(inst);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=174
Status	New

Calling free() (line 7257) on a variable that was not dynamically allocated (line 7257) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	7305	7305
Object	lang	lang

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	BOOL handle_SSH2_userauth_inforeq(PTInstVar pvar)

```
....
7305.        free(lang);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=175
Status	New

Calling free() (line 7567) on a variable that was not dynamically allocated (line 7567) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	7608	7608
Object	info	info

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	BOOL handle_SSH2_userauth_passwd_changereq(PTInstVar pvar)

```
....
7608.        free(info);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=176
Status	New

Calling free() (line 7567) on a variable that was not dynamically allocated (line 7567) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	7609	7609
Object	lang	lang

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL handle_SSH2_userauth_passwd_changereq(PTInstVar pvar)

```
....
7609.        free(lang);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=177
Status	New

Calling free() (line 7900) on a variable that was not dynamically allocated (line 7900) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	7953	7953
Object	cstring	cstring

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_open_failure(PTInstVar pvar)

```
....
7953.        free(cstring);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=178
Status	New

Calling free() (line 7966) on a variable that was not dynamically allocated (line 7966) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8011	8011
Object	rtype	rtype

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_client_global_request(PTInstVar pvar)

```
....
8011.        free(rtype);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=179
Status	New

Calling free() (line 8519) on a variable that was not dynamically allocated (line 8519) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8556	8556
Object	data	data

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static unsigned __stdcall ssh_scp_receive_thread(void *p)

```
....
8556.                                free(data);   // free!
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=180
Status	New

Calling free() (line 8519) on a variable that was not dynamically allocated (line 8519) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8571	8571
Object	data	data

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static unsigned __stdcall ssh_scp_receive_thread(void *p)

```
....
8571.                              free(data);   // free!
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=181
Status	New

Calling free() (line 8655) on a variable that was not dynamically allocated (line 8655) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8676	8676
Object	p	p

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void ssh2_scp_get_packetlist(Channel_t *c, unsigned char **buf, unsigned int *buflen)

```
....
8676.        free(p);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=182
Status	New

Calling free() (line 8689) on a variable that was not dynamically allocated (line 8689) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8699	8699
Object	old	old

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void ssh2_scp_free_packetlist(Channel_t *c)

```
....
8699.                free(old);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=183
Status New

Calling free() (line 9068) on a variable that was not dynamically allocated (line 9068) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	9149	9149
Object	listen_addr	listen_addr

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_channel_open(PTInstVar pvar)

```
....
9149.                free(listen_addr);
```

MemoryFree on StackVariable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=184
Status New

Calling free() (line 9068) on a variable that was not dynamically allocated (line 9068) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	9150	9150
Object	orig_addr	orig_addr

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_channel_open(PTInstVar pvar)

```
....
9150.               free(orig_addr);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=185
Status	New

Calling free() (line 9068) on a variable that was not dynamically allocated (line 9068) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	9164	9164
Object	orig_str	orig_str

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_channel_open(PTInstVar pvar)

```
....
9164.               free(orig_str);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=186
Status	New

Calling free() (line 9068) on a variable that was not dynamically allocated (line 9068) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	9224	9224
Object	ctype	ctype

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_channel_open(PTInstVar pvar)

```
....
9224.         free(ctype);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=187
Status	New

Calling free() (line 9289) on a variable that was not dynamically allocated (line 9289) in file TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c may result with a crash.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	9344	9344
Object	request	request

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_channel_request(PTInstVar pvar)

```
....
9344.         free(request);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=188
Status	New

Calling free() (line 812) on a variable that was not dynamically allocated (line 812) in file tmux@@tmux-3.1a-CVE-2020-27347-TP.c may result with a crash.

	Source	Destination
File	tmux@@tmux-3.1a-CVE-2020-27347-TP.c	tmux@@tmux-3.1a-CVE-2020-27347-TP.c
Line	827	827
Object	ictx	ictx

Code Snippet
File Name tmux@@tmux-3.1a-CVE-2020-27347-TP.c
Method input_free(struct window_pane *wp)

```
....
827.        free(ictx);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=189
Status	New

Calling free() (line 1044) on a variable that was not dynamically allocated (line 1044) in file tmux@@tmux-3.1a-CVE-2020-27347-TP.c may result with a crash.

	Source	Destination
File	tmux@@tmux-3.1a-CVE-2020-27347-TP.c	tmux@@tmux-3.1a-CVE-2020-27347-TP.c
Line	1054	1054
Object	reply	reply

Code Snippet
File Name tmux@@tmux-3.1a-CVE-2020-27347-TP.c
Method input_reply(struct input_ctx *ictx, const char *fmt, ...)

```
....
1054.       free(reply);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=190
Status	New

Calling free() (line 812) on a variable that was not dynamically allocated (line 812) in file tmux@@tmux-3.1a-CVE-2021-3520-FP.c may result with a crash.

	Source	Destination
File	tmux@@tmux-3.1a-CVE-2021-3520-FP.c	tmux@@tmux-3.1a-CVE-2021-3520-FP.c
Line	827	827
Object	ictx	ictx

Code Snippet
File Name tmux@@tmux-3.1a-CVE-2021-3520-FP.c
Method input_free(struct window_pane *wp)

```
....
827.        free(ictx);
```

MemoryFree on StackVariable\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=191
Status New

Calling free() (line 1044) on a variable that was not dynamically allocated (line 1044) in file tmux@@tmux-3.1a-CVE-2021-3520-FP.c may result with a crash.

	Source	Destination
File	tmux@@tmux-3.1a-CVE-2021-3520-FP.c	tmux@@tmux-3.1a-CVE-2021-3520-FP.c
Line	1054	1054
Object	reply	reply

Code Snippet
File Name tmux@@tmux-3.1a-CVE-2021-3520-FP.c
Method input_reply(struct input_ctx *ictx, const char *fmt, ...)

```
....
1054.        free(reply);
```

MemoryFree on StackVariable\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=192
Status New

Calling free() (line 812) on a variable that was not dynamically allocated (line 812) in file tmux@@tmux-3.1c-CVE-2021-3520-FP.c may result with a crash.

	Source	Destination
File	tmux@@tmux-3.1c-CVE-2021-3520-FP.c	tmux@@tmux-3.1c-CVE-2021-3520-FP.c
Line	827	827
Object	ictx	ictx

Code Snippet
File Name tmux@@tmux-3.1c-CVE-2021-3520-FP.c
Method input_free(struct window_pane *wp)

```
....
827.         free(ictx);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=193
Status	New

Calling free() (line 1044) on a variable that was not dynamically allocated (line 1044) in file tmux@@tmux-3.1c-CVE-2021-3520-FP.c may result with a crash.

	Source	Destination
File	tmux@@tmux-3.1c-CVE-2021-3520-FP.c	tmux@@tmux-3.1c-CVE-2021-3520-FP.c
Line	1054	1054
Object	reply	reply

Code Snippet
File Name tmux@@tmux-3.1c-CVE-2021-3520-FP.c
Method input_reply(struct input_ctx *ictx, const char *fmt, ...)

```
....
1054.        free(reply);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=194
Status	New

Calling free() (line 1075) on a variable that was not dynamically allocated (line 1075) in file tmux@@tmux-3.3-CVE-2021-3520-FP.c may result with a crash.

	Source	Destination
File	tmux@@tmux-3.3-CVE-2021-3520-FP.c	tmux@@tmux-3.3-CVE-2021-3520-FP.c

Line	1089	1089
Object	reply	reply

Code Snippet
File Name tmux@@tmux-3.3-CVE-2021-3520-FP.c
Method input_reply(struct input_ctx *ictx, const char *fmt, ...)

```
....
1089.        free(reply);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=195
Status	New

Calling free() (line 2461) on a variable that was not dynamically allocated (line 2461) in file tmux@@tmux-3.3-CVE-2021-3520-FP.c may result with a crash.

	Source	Destination
File	tmux@@tmux-3.3-CVE-2021-3520-FP.c	tmux@@tmux-3.3-CVE-2021-3520-FP.c
Line	2494	2494
Object	copy	copy

Code Snippet
File Name tmux@@tmux-3.3-CVE-2021-3520-FP.c
Method input_osc_parse_colour(const char *p)

```
....
2494.              free(copy);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=196
Status	New

Calling free() (line 610) on a variable that was not dynamically allocated (line 610) in file tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c may result with a crash.

	Source	Destination
File	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Line	724	724

Object	mnt_opts	mnt_opts

Code Snippet
File Name tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method int fuse_kern_mount(const char *mountpoint, struct fuse_args *args)

```
....
724.        free(mnt_opts);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=197
Status	New

Calling free() (line 610) on a variable that was not dynamically allocated (line 610) in file tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c may result with a crash.

	Source	Destination
File	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Line	724	724
Object	mnt_opts	mnt_opts

Code Snippet
File Name tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method int fuse_kern_mount(const char *mountpoint, struct fuse_args *args)

```
....
724.        free(mnt_opts);
```

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=1030073&projectid=30062&pathid=198
Status	New

The function alloc_size in tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c at line 53 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	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Line	56	56
Object	alloc_size	alloc_size

Code Snippet
File Name tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Method TfLiteIntArray* TfLiteIntArrayCreate(int size) {

```
....
56.     TfLiteIntArray* ret = (TfLiteIntArray*)malloc(alloc_size);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=199
Status	New

The function alloc_size in tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c at line 55 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	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Line	58	58
Object	alloc_size	alloc_size

Code Snippet
File Name tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Method TfLiteIntArray* TfLiteIntArrayCreate(int size) {

```
....
58.     TfLiteIntArray* ret = (TfLiteIntArray*)malloc(alloc_size);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=200
Status	New

The function buflen in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c at line 8336 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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8352	8352
Object	buflen	buflen

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static unsigned __stdcall ssh_scp_thread(void *p)

```
....
8352.       buf = malloc(buflen);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=201
Status	New

The function _cbBuffer in ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c at line 862 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	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Line	879	879
Object	_cbBuffer	_cbBuffer

Code Snippet
File Name ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Method char *JSON_EncodeObject(JSOBJ obj, JSONObjectEncoder *enc, char *_buffer, size_t _cbBuffer)

```
....
879.      enc->start = (char *) enc->malloc (_cbBuffer);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=202
Status	New

The function _cbBuffer in ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c at line 862 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	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Line	879	879
Object	_cbBuffer	_cbBuffer

Code Snippet
File Name ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Method char *JSON_EncodeObject(JSOBJ obj, JSONObjectEncoder *enc, char *_buffer, size_t _cbBuffer)

```
....
879.      enc->start = (char *) enc->malloc (_cbBuffer);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=203
Status	New

The function _cbBuffer in ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c at line 866 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	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Line	883	883
Object	_cbBuffer	_cbBuffer

Code Snippet
File Name ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Method char *JSON_EncodeObject(JSOBJ obj, JSONObjectEncoder *enc, char *_buffer, size_t _cbBuffer)

```
....
883.      enc->start = (char *) enc->malloc (_cbBuffer);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30

	062&pathid=204
Status	New

The function _cbBuffer in ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c at line 865 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	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Line	882	882
Object	_cbBuffer	_cbBuffer

Code Snippet

File Name	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Method	char *JSON_EncodeObject(JSOBJ obj, JSONObjectEncoder *enc, char *_buffer, size_t _cbBuffer)

```
....
882.        enc->start = (char *) enc->malloc (_cbBuffer);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=205
Status	New

The function _cbBuffer in ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c at line 865 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	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Line	882	882
Object	_cbBuffer	_cbBuffer

Code Snippet

File Name	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Method	char *JSON_EncodeObject(JSOBJ obj, JSONObjectEncoder *enc, char *_buffer, size_t _cbBuffer)

```
....
882.        enc->start = (char *) enc->malloc (_cbBuffer);
```

Wrong Size t Allocation\Path 9:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=206
Status	New

The function size in tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c at line 346 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	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	359	359
Object	size	size

Code Snippet

File Name	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method	static bool eventlog_from_file(tpm2_eventlog_context *evctx, const char *file_path) {

```
....
359.        uint8_t *eventlog = calloc(1, size);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=207
Status	New

The function size in tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c at line 346 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	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	359	359
Object	size	size

Code Snippet

File Name	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method	static bool eventlog_from_file(tpm2_eventlog_context *evctx, const char *file_path) {

```
....
359.        uint8_t *eventlog = calloc(1, size);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=208
Status	New

The function len in tmux@@tmux-3.1a-CVE-2020-27347-TP.c at line 2486 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	tmux@@tmux-3.1a-CVE-2020-27347-TP.c	tmux@@tmux-3.1a-CVE-2020-27347-TP.c
Line	2536	2536
Object	len	len

Code Snippet
File Name tmux@@tmux-3.1a-CVE-2020-27347-TP.c
Method input_osc_52(struct input_ctx *ictx, const char *p)

```
....
2536.        out = xmalloc(len);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=209
Status	New

The function len in tmux@@tmux-3.1a-CVE-2021-3520-FP.c at line 2486 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	tmux@@tmux-3.1a-CVE-2021-3520-FP.c	tmux@@tmux-3.1a-CVE-2021-3520-FP.c
Line	2536	2536
Object	len	len

Code Snippet
File Name tmux@@tmux-3.1a-CVE-2021-3520-FP.c
Method input_osc_52(struct input_ctx *ictx, const char *p)

```
....
2536.        out = xmalloc(len);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=210
Status	New

The function len in tmux@@tmux-3.1c-CVE-2021-3520-FP.c at line 2491 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	tmux@@tmux-3.1c-CVE-2021-3520-FP.c	tmux@@tmux-3.1c-CVE-2021-3520-FP.c
Line	2541	2541
Object	len	len

Code Snippet
File Name tmux@@tmux-3.1c-CVE-2021-3520-FP.c
Method input_osc_52(struct input_ctx *ictx, const char *p)

```
....
2541.         out = xmalloc(len);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=211
Status	New

The function outlen in tmux@@tmux-3.3-CVE-2021-3520-FP.c at line 2776 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	tmux@@tmux-3.3-CVE-2021-3520-FP.c	tmux@@tmux-3.3-CVE-2021-3520-FP.c
Line	2784	2784
Object	outlen	outlen

Code Snippet
File Name tmux@@tmux-3.3-CVE-2021-3520-FP.c
Method input_reply_clipboard(struct bufferevent *bev, const char *buf, size_t len,

```
....
2784.               out = xmalloc(outlen);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=212
Status	New

The function len in tmux@@tmux-3.3-CVE-2021-3520-FP.c at line 2686 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	tmux@@tmux-3.3-CVE-2021-3520-FP.c	tmux@@tmux-3.3-CVE-2021-3520-FP.c
Line	2724	2724
Object	len	len

Code Snippet

File Name	tmux@@tmux-3.3-CVE-2021-3520-FP.c
Method	input_osc_52(struct input_ctx *ictx, const char *p)

```
....
2724.        out = xmalloc(len);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=213
Status	New

The function available in tmux@@tmux-3.1a-CVE-2020-27347-TP.c at line 1144 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	tmux@@tmux-3.1a-CVE-2020-27347-TP.c	tmux@@tmux-3.1a-CVE-2020-27347-TP.c
Line	1155	1155
Object	available	available

Code Snippet

File Name	tmux@@tmux-3.1a-CVE-2020-27347-TP.c
Method	input_input(struct input_ctx *ictx)

```
....
1155.            ictx->input_buf = xrealloc(ictx->input_buf,
available);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=214
Status	New

The function available in tmux@@tmux-3.1a-CVE-2021-3520-FP.c at line 1144 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	tmux@@tmux-3.1a-CVE-2021-3520-FP.c	tmux@@tmux-3.1a-CVE-2021-3520-FP.c
Line	1155	1155
Object	available	available

Code Snippet

File Name	tmux@@tmux-3.1a-CVE-2021-3520-FP.c
Method	input_input(struct input_ctx *ictx)

```
....
1155.           ictx->input_buf = xrealloc(ictx->input_buf,
available);
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=215
Status	New

The function available in tmux@@tmux-3.1c-CVE-2021-3520-FP.c at line 1144 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	tmux@@tmux-3.1c-CVE-2021-3520-FP.c	tmux@@tmux-3.1c-CVE-2021-3520-FP.c
Line	1155	1155
Object	available	available

Code Snippet

File Name	tmux@@tmux-3.1c-CVE-2021-3520-FP.c
Method	input_input(struct input_ctx *ictx)

```
....
1155.           ictx->input_buf = xrealloc(ictx->input_buf,
available);
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=216
Status	New

The function available in tmux@@tmux-3.3-CVE-2021-3520-FP.c at line 1179 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	tmux@@tmux-3.3-CVE-2021-3520-FP.c	tmux@@tmux-3.3-CVE-2021-3520-FP.c
Line	1190	1190
Object	available	available

Code Snippet
File Name tmux@@tmux-3.3-CVE-2021-3520-FP.c
Method input_input(struct input_ctx *ictx)

```
....
1190.           ictx->input_buf = xrealloc(ictx->input_buf,
available);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=217
Status	New

The function newSize in ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c at line 295 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	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c
Line	334	334
Object	newSize	newSize

Code Snippet

File Name	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c
Method	static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
334.        ds->escStart = (wchar_t *) ds->dec->malloc(newSize *
sizeof(wchar_t));
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=218
Status	New

The function newSize in ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c at line 295 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	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c
Line	334	334
Object	newSize	newSize

Code Snippet

File Name	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c
Method	static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
334.        ds->escStart = (wchar_t *) ds->dec->malloc(newSize *
sizeof(wchar_t));
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=219
Status	New

The function newSize in ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c at line 307 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	ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c

Line	346	346
Object	newSize	newSize

Code Snippet
File Name ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
346.        ds->escStart = (wchar_t *) ds->dec->malloc(newSize *
sizeof(wchar_t));
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=220
Status	New

The function newSize in ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c at line 307 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	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c
Line	346	346
Object	newSize	newSize

Code Snippet
File Name ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
346.        ds->escStart = (wchar_t *) ds->dec->malloc(newSize *
sizeof(wchar_t));
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=221
Status	New

The function newSize in ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c at line 295 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	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c
Line	319	319
Object	newSize	newSize

Code Snippet
File Name ultrajson@@ultrajson-2.0.0-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
319.         escStart = (wchar_t *)ds->dec->realloc(ds->escStart, newSize
* sizeof(wchar_t));
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=222
Status	New

The function newSize in ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c at line 295 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	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c
Line	319	319
Object	newSize	newSize

Code Snippet
File Name ultrajson@@ultrajson-3.1.0-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
319.         escStart = (wchar_t *)ds->dec->realloc(ds->escStart, newSize
* sizeof(wchar_t));
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=223
Status	New

The function newSize in ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c at line 307 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	ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c
Line	331	331
Object	newSize	newSize

Code Snippet
File Name ultrajson@@ultrajson-4.0.2-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
331.        escStart = (wchar_t *)ds->dec->realloc(ds->escStart, newSize
* sizeof(wchar_t));
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=224
Status	New

The function newSize in ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c at line 307 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	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c
Line	331	331
Object	newSize	newSize

Code Snippet
File Name ultrajson@@ultrajson-4.1.0-CVE-2022-31117-TP.c
Method static FASTCALL_ATTR JSOBJ FASTCALL_MSVC decode_string (struct DecoderState *ds)

```
....
331.        escStart = (wchar_t *)ds->dec->realloc(ds->escStart, newSize
* sizeof(wchar_t));
```

Wrong Size t Allocation\Path 28:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=225
Status	New

The function size in tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c at line 117 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	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Line	131	131
Object	size	size

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Method	static TPM2B_ATTEST *message_from_file(const char *msg_file_path) {

```
....
131.      TPM2B_ATTEST *msg = (TPM2B_ATTEST *) calloc(1,
sizeof(TPM2B_ATTEST) + size);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=226
Status	New

The function size in tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c at line 117 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	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Line	131	131
Object	size	size

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Method	static TPM2B_ATTEST *message_from_file(const char *msg_file_path) {

```
....
131.      TPM2B_ATTEST *msg = (TPM2B_ATTEST *) calloc(1,
sizeof(TPM2B_ATTEST) + size);
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=227
Status	New

The function size in tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c at line 117 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	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Line	131	131
Object	size	size

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Method static TPM2B_ATTEST *message_from_file(const char *msg_file_path) {

```
....
131.      TPM2B_ATTEST *msg = (TPM2B_ATTEST *) calloc(1,
sizeof(TPM2B_ATTEST) + size);
```

Wrong Size t Allocation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=228
Status	New

The function size in tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c at line 117 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	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Line	131	131
Object	size	size

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Method static TPM2B_ATTEST *message_from_file(const char *msg_file_path) {

```
....
131.       TPM2B_ATTEST *msg = (TPM2B_ATTEST *) calloc(1,
sizeof(TPM2B_ATTEST) + size);
```

Wrong Size t Allocation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=229
Status	New

The function size in tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c at line 117 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	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Line	131	131
Object	size	size

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Method static TPM2B_ATTEST *message_from_file(const char *msg_file_path) {

```
....
131.       TPM2B_ATTEST *msg = (TPM2B_ATTEST *) calloc(1,
sizeof(TPM2B_ATTEST) + size);
```

Wrong Size t Allocation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=230
Status	New

The function size in tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c at line 117 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	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Line	131	131
Object	size	size

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Method static TPM2B_ATTEST *message_from_file(const char *msg_file_path) {

```
....
131.       TPM2B_ATTEST *msg = (TPM2B_ATTEST *) calloc(1,
sizeof(TPM2B_ATTEST) + size);
```

Wrong Size t Allocation\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=231
Status	New

The function size in tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c at line 150 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	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	164	164
Object	size	size

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method static TPM2B_ATTEST *message_from_file(const char *msg_file_path) {

```
....
164.       TPM2B_ATTEST *msg = (TPM2B_ATTEST *) calloc(1,
sizeof(TPM2B_ATTEST) + size);
```

Wrong Size t Allocation\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=232
Status	New

The function size in tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c at line 150 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	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	164	164

Object	size	size

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method static TPM2B_ATTEST *message_from_file(const char *msg_file_path) {

```
....
164.       TPM2B_ATTEST *msg = (TPM2B_ATTEST *) calloc(1,
sizeof(TPM2B_ATTEST) + size);
```

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=1030073&projectid=30062&pathid=592
Status	New

	Source	Destination
File	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Line	56	56
Object	ret	ret

Code Snippet
File Name tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Method TfLiteIntArray* TfLiteIntArrayCreate(int size) {

```
....
56.    TfLiteIntArray* ret = (TfLiteIntArray*)malloc(alloc_size);
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=593
Status	New

	Source	Destination
File	tensorflow@@tensorflow-v2.8.0-rc1-	tensorflow@@tensorflow-v2.8.0-rc1-

	CVE-2021-29605-FP.c	CVE-2021-29605-FP.c
Line	89	89
Object	ret	ret

Code Snippet
File Name tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Method TfLiteFloatArray* TfLiteFloatArrayCreate(int size) {

```
....
89.     TfLiteFloatArray* ret =
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=594
Status	New

	Source	Destination
File	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Line	58	58
Object	ret	ret

Code Snippet
File Name tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Method TfLiteIntArray* TfLiteIntArrayCreate(int size) {

```
....
58.     TfLiteIntArray* ret = (TfLiteIntArray*)malloc(alloc_size);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=595
Status	New

	Source	Destination
File	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Line	91	91
Object	ret	ret

Code Snippet

File Name	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Method	TfLiteFloatArray* TfLiteFloatArrayCreate(int size) {

```
....
91.    TfLiteFloatArray* ret =
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=596
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1337	1337
Object	item	item

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void enque_handlers(PTInstVar pvar, int num_msgs,

```
....
1337.            SSHPacketHandlerItem *item =
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=597
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8782	8782
Object	newdata	newdata

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static BOOL SSH2_scp_fromremote(PTInstVar pvar, Channel_t *c, unsigned char *data, unsigned int buflen)

```
....
8782.            unsigned char *newdata = malloc(buflen);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=598
Status	New

	Source	Destination
File	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Line	218	218
Object	raw	raw

Code Snippet
File Name tensorflow@@tensorflow-v2.8.0-rc1-CVE-2021-29605-FP.c
Method void TfLiteTensorRealloc(size_t num_bytes, TfLiteTensor* tensor) {

```
....
218.      tensor->data.raw = (char*)malloc(num_bytes);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=599
Status	New

	Source	Destination
File	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Line	220	220
Object	raw	raw

Code Snippet
File Name tensorflow@@tensorflow-v2.9.0-rc2-CVE-2021-29605-FP.c
Method void TfLiteTensorRealloc(size_t num_bytes, TfLiteTensor* tensor) {

```
....
220.      tensor->data.raw = (char*)malloc(num_bytes);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=600

Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	611	611
Object	dp	dp

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void push_memdump(char *name, char *desc, char *data, int len)

```
....
611.         dp = malloc(len);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=601
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5414	5414
Object	session_id	session_id

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL ssh2_kex_finish(PTInstVar pvar, char *hash, int hashlen, BIGNUM *share_key, Key *hostkey, char *signature, int siglen)

```
....
5414.            pvar->session_id = malloc(pvar->session_id_len);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=602
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Line	5489	5489
Object	payload	payload

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL store_contents_for_known_hosts(PTInstVar pvar, enum ssh_kex_known_hosts kex_type, UINT_PTR offset)

```
....
5489.       pvar->contents_after_known_hosts.payload = malloc(pvar->ssh_state.payloadlen);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=603
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8634	8634
Object	p	p

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void ssh2_scp_add_packetlist(Channel_t *c, unsigned char *buf, unsigned int buflen)

```
....
8634.       p = malloc(sizeof(PacketList_t));
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=604
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Line	310	310
Object	buffer	buffer

Code Snippet

File Name	tpm2-software@@tpm2-tss-2.4.1-CVE-2024-29040-TP.c
Method	ifapi_json_UINT8_ARY_deserialize(

```
....
310.        out->buffer = malloc(out->size);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=605
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Line	316	316
Object	buffer	buffer

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.0.1-CVE-2024-29040-TP.c
Method	ifapi_json_UINT8_ARY_deserialize(

```
....
316.        out->buffer = malloc(out->size);
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=606
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Line	317	317
Object	buffer	buffer

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.1.0-CVE-2024-29040-TP.c
Method	ifapi_json_UINT8_ARY_deserialize(

```
....
317.        out->buffer = malloc(out->size);
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=607
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Line	361	361
Object	buffer	buffer

Code Snippet

File Name tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c

Method ifapi_json_UINT8_ARY_deserialize(

```
....
361.        out->buffer = malloc(out->size);
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=608
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.1-CVE-2024-29040-TP.c
Line	361	361
Object	buffer	buffer

Code Snippet

File Name tpm2-software@@tpm2-tss-3.2.1-CVE-2024-29040-TP.c

Method ifapi_json_UINT8_ARY_deserialize(

```
....
361.        out->buffer = malloc(out->size);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=609

Status	New

	Source	Destination
File	tpm2-software@@tpm2-tss-4.1.0-rc0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-4.1.0-rc0-CVE-2024-29040-TP.c
Line	348	348
Object	buffer	buffer

Code Snippet
File Name tpm2-software@@tpm2-tss-4.1.0-rc0-CVE-2024-29040-TP.c
Method ifapi_json_UINT8_ARY_deserialize(

```
....
348.       out->buffer = malloc(out->size);
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=610
Status	New

	Source	Destination
File	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Line	879	879
Object	start	start

Code Snippet
File Name ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Method char *JSON_EncodeObject(JSOBJ obj, JSONObjectEncoder *enc, char *_buffer, size_t _cbBuffer)

```
....
879.       enc->start = (char *) enc->malloc (_cbBuffer);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=611
Status	New

	Source	Destination
File	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c

Line	139	139
Object	start	start

Code Snippet

File Name	ultrajson@@ultrajson-2.0.0-CVE-2021-45958-TP.c
Method	static void Buffer_Realloc (JSONObjectEncoder *enc, size_t cbNeeded)

```
....
139.        enc->start = (char *) enc->malloc (newSize);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=612
Status	New

	Source	Destination
File	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Line	879	879
Object	start	start

Code Snippet

File Name	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Method	char *JSON_EncodeObject(JSOBJ obj, JSONObjectEncoder *enc, char *_buffer, size_t _cbBuffer)

```
....
879.        enc->start = (char *) enc->malloc (_cbBuffer);
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=613
Status	New

	Source	Destination
File	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Line	139	139
Object	start	start

Code Snippet

File Name	ultrajson@@ultrajson-3.1.0-CVE-2021-45958-TP.c
Method	static void Buffer_Realloc (JSONObjectEncoder *enc, size_t cbNeeded)

```
....
139.        enc->start = (char *) enc->malloc (newSize);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=614
Status	New

	Source	Destination
File	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Line	883	883
Object	start	start

Code Snippet

File Name	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Method	char *JSON_EncodeObject(JSOBJ obj, JSONObjectEncoder *enc, char *_buffer, size_t _cbBuffer)

```
....
883.        enc->start = (char *) enc->malloc (_cbBuffer);
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=615
Status	New

	Source	Destination
File	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Line	139	139
Object	start	start

Code Snippet

File Name	ultrajson@@ultrajson-4.0.2-CVE-2021-45958-TP.c
Method	static void Buffer_Realloc (JSONObjectEncoder *enc, size_t cbNeeded)

```
....
139.        enc->start = (char *) enc->malloc (newSize);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=616
Status	New

	Source	Destination
File	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Line	882	882
Object	start	start

Code Snippet

File Name	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Method	char *JSON_EncodeObject(JSOBJ obj, JSONObjectEncoder *enc, char *_buffer, size_t _cbBuffer)

```
....
882.      enc->start = (char *) enc->malloc (_cbBuffer);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=617
Status	New

	Source	Destination
File	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Line	138	138
Object	start	start

Code Snippet

File Name	ultrajson@@ultrajson-4.1.0-CVE-2021-45958-TP.c
Method	static void Buffer_Realloc (JSONObjectEncoder *enc, size_t cbNeeded)

```
....
138.      enc->start = (char *) enc->malloc (newSize);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30

	062&pathid=618
Status	New

	Source	Destination
File	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Line	882	882
Object	start	start

Code Snippet
File Name ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Method char *JSON_EncodeObject(JSOBJ obj, JSONObjectEncoder *enc, char *_buffer, size_t _cbBuffer)

```
....
882.      enc->start = (char *) enc->malloc (_cbBuffer);
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=619
Status	New

	Source	Destination
File	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c	ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Line	138	138
Object	start	start

Code Snippet
File Name ultrajson@@ultrajson-4.3.0-CVE-2021-45958-TP.c
Method static void Buffer_Realloc (JSONObjectEncoder *enc, size_t cbNeeded)

```
....
138.      enc->start = (char *) enc->malloc (newSize);
```

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=1030073&projectid=30062&pathid=897
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Line	214	280
Object	msg	msg

Code Snippet
File Name tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Method static tool_rc init(void) {

```
....
214.        TPM2B_ATTEST *msg = NULL;
....
280.        bool res = tpm2_openssl_hash_compute_data(ctx.halg, msg-
>attestationData,
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=898
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Line	214	281
Object	msg	msg

Code Snippet
File Name tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Method static tool_rc init(void) {

```
....
214.      TPM2B_ATTEST *msg = NULL;
....
281.              msg->size, &ctx.msg_hash);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=899
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Line	214	280
Object	msg	msg

Code Snippet
File Name tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Method static tool_rc init(void) {

```
....
214.      TPM2B_ATTEST *msg = NULL;
....
280.      bool res = tpm2_openssl_hash_compute_data(ctx.halg, msg->attestationData,
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=900
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Line	214	281

Object	msg	msg

Code Snippet
File Name tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Method static tool_rc init(void) {

```
....
214.      TPM2B_ATTEST *msg = NULL;
....
281.                msg->size, &ctx.msg_hash);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=901
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Line	214	283
Object	msg	msg

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Method static tool_rc init(void) {

```
....
214.      TPM2B_ATTEST *msg = NULL;
....
283.      bool res = tpm2_openssl_hash_compute_data(ctx.halg, msg-
>attestationData,
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=902
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Line	214	284
Object	msg	msg

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Method static tool_rc init(void) {

```
....
214.        TPM2B_ATTEST *msg = NULL;
....
284.                msg->size, &ctx.msg_hash);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=903
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Line	214	283
Object	msg	msg

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Method static tool_rc init(void) {

```
....
214.        TPM2B_ATTEST *msg = NULL;
....
283.        bool res = tpm2_openssl_hash_compute_data(ctx.halg, msg-
>attestationData,
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=904
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Line	214	284
Object	msg	msg

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Method static tool_rc init(void) {

```
....
214.        TPM2B_ATTEST *msg = NULL;
....
284.                msg->size, &ctx.msg_hash);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=905
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Line	214	283
Object	msg	msg

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Method static tool_rc init(void) {

```
....
214.        TPM2B_ATTEST *msg = NULL;
....
283.        bool res = tpm2_openssl_hash_compute_data(ctx.halg, msg-
>attestationData,
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=906
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Line	214	284
Object	msg	msg

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Method	static tool_rc init(void) {

```
....
214.        TPM2B_ATTEST *msg = NULL;
....
284.                msg->size, &ctx.msg_hash);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=907
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Line	214	283
Object	msg	msg

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Method	static tool_rc init(void) {

```
....
214.       TPM2B_ATTEST *msg = NULL;
....
283.       bool res = tpm2_openssl_hash_compute_data(ctx.halg, msg-
>attestationData,
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=908
Status	New

The variable declared in msg at tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c in line 205 is not initialized when it is used by msg at tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c in line 205.

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Line	214	284
Object	msg	msg

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Method static tool_rc init(void) {

```
....
214.       TPM2B_ATTEST *msg = NULL;
....
284.               msg->size, &ctx.msg_hash);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=909
Status	New

The variable declared in pkey at tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c in line 57 is not initialized when it is used by pkey_ctx at tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c in line 57.

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	63	81

Object	pkey	pkey_ctx

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method static bool verify(void) {

```
....
63.       EVP_PKEY *pkey = NULL;
....
81.       pkey_ctx = EVP_PKEY_CTX_new(pkey, NULL);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=910
Status	New

The variable declared in pkey at tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c in line 57 is not initialized when it is used by pkey_ctx at tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c in line 57.

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	63	81
Object	pkey	pkey_ctx

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method static bool verify(void) {

```
....
63.       EVP_PKEY *pkey = NULL;
....
81.       pkey_ctx = EVP_PKEY_CTX_new(pkey, NULL);
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=911
Status	New

The variable declared in next at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 241 is not initialized when it is used by next at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 241.

	Source	Destination

File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	255	263
Object	next	next

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void ssh2_channel_add_bufchain(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen)

```
....
255.        p->next = NULL;
....
263.                old->next = p;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=912
Status	New

The variable declared in replacement at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 1384 is not initialized when it is used by replacement at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 1384.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1401	1397
Object	replacement	replacement

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void deque_handlers(PTInstVar pvar, int message)

```
....
1401.                           replacement = NULL;
....
1397.                   SSHPacketHandlerItem *replacement =
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=913
Status	New

The variable declared in dh at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 5008 is not initialized when it is used by kexdh at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 5008.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5010	5056
Object	dh	kexdh

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void SSH2_dh_kex_init(PTInstVar pvar)

```
....
5010.       DH *dh = NULL;
....
5056.       pvar->kexdh = dh;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=914
Status	New

The variable declared in c at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by c at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	3526
Object	c	c

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.              c = NULL;
....
3526.   void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c,
unsigned char *buf, unsigned int buflen, int retry)
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=915
Status	New

The variable declared in c at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by c at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	3568
Object	c	c

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.                c = NULL;
....
3568.                buffer_put_int(msg, c->remote_id);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=916
Status	New

The variable declared in c at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by c at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	3579
Object	c	c

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.               c = NULL;
....
3579.                                 "local:%d remote:%d len:%d",
__FUNCTION__, c->self_id, c->remote_id, buflen);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=917
Status	New

The variable declared in next at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 8627 is not initialized when it is used by next at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 8627.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8639	8647
Object	next	next

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void ssh2_scp_add_packetlist(Channel_t *c, unsigned char *buf, unsigned int buflen)

```
....
8639.       p->next = NULL;
....
8647.               old->next = p;
```

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=1030073&projectid=30062&pathid=233
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8336 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8402	8402
Object	AssignExpr	AssignExpr

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static unsigned __stdcall ssh_scp_thread(void *p)

```
....
8402.                  rate = (int)(100 * total_size / c-
>scp.filestat.st_size);
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=234
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8336 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8413	8413
Object	AssignExpr	AssignExpr

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static unsigned __stdcall ssh_scp_thread(void *p)

```
....
8413.                              rate = (int)(total_size / elapsed);
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=235
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8336 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8410	8410
Object	AssignExpr	AssignExpr

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static unsigned __stdcall ssh_scp_thread(void *p)

```
....
8410.                   elapsed = (GetTickCount() - stime) / 1000;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=236
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8519 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8582	8582
Object	AssignExpr	AssignExpr

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static unsigned __stdcall ssh_scp_receive_thread(void *p)

```
....
8582.                               elapsed = (GetTickCount() - stime) / 1000;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=237
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2486 of tmux@@tmux-3.1a-CVE-2020-27347-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tmux@@tmux-3.1a-CVE-2020-27347-TP.c	tmux@@tmux-3.1a-CVE-2020-27347-TP.c
Line	2511	2511
Object	AssignExpr	AssignExpr

Code Snippet
File Name tmux@@tmux-3.1a-CVE-2020-27347-TP.c
Method input_osc_52(struct input_ctx *ictx, const char *p)

```
....
2511.                   outlen = 4 * ((len + 2) / 3) + 1;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=238
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2486 of tmux@@tmux-3.1a-CVE-2021-3520-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tmux@@tmux-3.1a-CVE-2021-3520-FP.c	tmux@@tmux-3.1a-CVE-2021-3520-FP.c
Line	2511	2511
Object	AssignExpr	AssignExpr

Code Snippet
File Name tmux@@tmux-3.1a-CVE-2021-3520-FP.c
Method input_osc_52(struct input_ctx *ictx, const char *p)

```
....
2511.                   outlen = 4 * ((len + 2) / 3) + 1;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=239
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2491 of tmux@@tmux-3.1c-CVE-2021-3520-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	tmux@@tmux-3.1c-CVE-2021-3520-FP.c	tmux@@tmux-3.1c-CVE-2021-3520-FP.c
Line	2516	2516
Object	AssignExpr	AssignExpr

Code Snippet
File Name tmux@@tmux-3.1c-CVE-2021-3520-FP.c
Method input_osc_52(struct input_ctx *ictx, const char *p)

```
....
2516.                  outlen = 4 * ((len + 2) / 3) + 1;
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

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=1030073&projectid=30062&pathid=620
Status	New

The variable declared in output_t at tensorflow@@tensorflow-v2.7.0-rc1-CVE-2022-41886-TP.c in line 52 is not initialized when it is used by output_t at tensorflow@@tensorflow-v2.7.0-rc1-CVE-2022-41886-TP.c in line 52.

	Source	Destination
File	tensorflow@@tensorflow-v2.7.0-rc1-CVE-2022-41886-TP.c	tensorflow@@tensorflow-v2.7.0-rc1-CVE-2022-41886-TP.c
Line	98	104
Object	output_t	output_t

Code Snippet
File Name tensorflow@@tensorflow-v2.7.0-rc1-CVE-2022-41886-TP.c
Method void DoImageProjectiveTransformOp(OpKernelContext* ctx,

```
....
98.     Tensor* output_t;
....
104.     auto output = output_t->tensor<T, 4>();
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=621
Status	New

The variable declared in output_t at tensorflow@@tensorflow-v2.8.0-rc1-CVE-2022-41886-TP.c in line 52 is not initialized when it is used by output_t at tensorflow@@tensorflow-v2.8.0-rc1-CVE-2022-41886-TP.c in line 52.

	Source	Destination
File	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2022-41886-TP.c	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2022-41886-TP.c
Line	98	104
Object	output_t	output_t

Code Snippet

File Name	tensorflow@@tensorflow-v2.8.0-rc1-CVE-2022-41886-TP.c
Method	void DoImageProjectiveTransformOp(OpKernelContext* ctx,

```
....
98.     Tensor* output_t;
....
104.      auto output = output_t->tensor<T, 4>();
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=622
Status	New

The variable declared in output_t at tensorflow@@tensorflow-v2.9.0-rc2-CVE-2022-41886-TP.c in line 52 is not initialized when it is used by output_t at tensorflow@@tensorflow-v2.9.0-rc2-CVE-2022-41886-TP.c in line 52.

	Source	Destination
File	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2022-41886-TP.c	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2022-41886-TP.c
Line	98	104
Object	output_t	output_t

Code Snippet

File Name	tensorflow@@tensorflow-v2.9.0-rc2-CVE-2022-41886-TP.c
Method	void DoImageProjectiveTransformOp(OpKernelContext* ctx,

```
....
98.     Tensor* output_t;
....
104.     auto output = output_t->tensor<T, 4>();
```

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=1030073&projectid=30062&pathid=591
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8571	8556
Object	data	data

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static unsigned __stdcall ssh_scp_receive_thread(void *p)

```
....
8571.                               free(data);  // free!
....
8556.                                     free(data);  // free!
```

Use of a One Way Hash without a Salt

Query Path:
CPP\Cx\CPP Medium Threat\Use of a One Way Hash without a Salt Version:1

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-13 Cryptographic Protection (P1)

Description

Use of a One Way Hash without a Salt\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=623

Status	New

The application protects passwords with MD5 in handle_rsa_challenge, of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c at line 2567, using a cryptographic hash session_buf. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2630	2630
Object	session_buf	MD5

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_rsa_challenge(PTInstVar pvar)

```
....
2630.                   MD5(session_buf, session_buf_len, session_id);
```

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=1030073&projectid=30062&pathid=626
Status	New

The SSH_agent_response method calls the strncpy_s function, at line 9429 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	9460	9460
Object	strncpy_s	strncpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL SSH_agent_response(PTInstVar pvar, Channel_t *c, int local_channel_num,

```
....
9460.                        strncpy_s(title, sizeof(title), pvar->ts-
>UIMsg, _TRUNCATE);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=627
Status	New

The ssh2_channel_delete method calls the remove function, at line 313 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	345	345
Object	remove	remove

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void ssh2_channel_delete(Channel_t *c)

```
....
345.                              remove(c->scp.localfilefull);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=628
Status	New

The grab_payload method calls the _snprintf_s function, at line 717 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	730	730
Object	_snprintf_s	_snprintf_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static BOOL grab_payload(PTInstVar pvar, int num_bytes)

```
....
730.                    _snprintf_s(buf, sizeof(buf), _TRUNCATE, pvar-
>ts->UIMsg,
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=629
Status	New

The grab_payload_limited method calls the _snprintf_s function, at line 740 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	754	754
Object	_snprintf_s	_snprintf_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static BOOL grab_payload_limited(PTInstVar pvar, int num_bytes)

```
....
754.                    _snprintf_s(buf, sizeof(buf), _TRUNCATE, pvar-
>ts->UIMsg,
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=630
Status	New

The get_bytearray_from_payload method calls the memcpy_s function, at line 778 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	787	787

Object	memcpy_s	memcpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static PayloadStat get_bytearray_from_payload(PTInstVar pvar, unsigned char *buff, unsigned int len)

```
....
787.        memcpy_s(buff, len, data, len);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=631
Status	New

The get_string_from_payload method calls the memcpy_s function, at line 804 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	822	822
Object	memcpy_s	memcpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static PayloadStat get_string_from_payload(

```
....
822.            memcpy_s(buff, bufflen, data, size);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=632
Status	New

The get_string_from_payload method calls the memcpy_s function, at line 804 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-	TeraTermProject@@teraterm-teraterm-

	4_106-CVE-2023-48795-TP.c	4_106-CVE-2023-48795-TP.c
Line	829	829
Object	memcpy_s	memcpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static PayloadStat get_string_from_payload(

```
....
829.                memcpy_s(buff, bufflen, data, bufflen);
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=633
Status New

The get_string_from_payload method calls the memcpy_s function, at line 804 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	839	839
Object	memcpy_s	memcpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static PayloadStat get_string_from_payload(

```
....
839.                memcpy_s(buff, bufflen, data, bufflen);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=634
Status New

The send_packet_blocking method calls the _snprintf_s function, at line 1089 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1126	1126
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL send_packet_blocking(PTInstVar pvar, char *data, int len)

```
....
1126.       _snprintf_s(buf, sizeof(buf), _TRUNCATE, pvar->ts->UIMsg,
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=635
Status	New

The handle_debug method calls the _snprintf_s function, at line 1537 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1573	1573
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_debug(PTInstVar pvar)

```
....
1573.       _snprintf_s(buf, sizeof(buf), _TRUNCATE, "DEBUG message from
server: %s",
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=636
Status	New

The handle_disconnect method calls the strncpy_s function, at line 1583 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1628	1628
Object	strncpy_s	strncpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_disconnect(PTInstVar pvar)

```
....
1628.           strncpy_s(uimsg, sizeof(uimsg), pvar->ts->UIMsg,
_TRUNCATE);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=637
Status	New

The handle_disconnect method calls the _snprintf_s function, at line 1583 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1635	1635
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_disconnect(PTInstVar pvar)

```
....
1635.           _snprintf_s(buf, sizeof(buf), _TRUNCATE,
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=638
Status	New

The handle_disconnect method calls the _snprintf_s function, at line 1583 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1641	1641
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_disconnect(PTInstVar pvar)

```
....
1641.                _snprintf_s(buf, sizeof(buf), _TRUNCATE,
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=639
Status	New

The SSH_handle_server_ID method calls the strncpy_s function, at line 1943 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1959	1959
Object	strncpy_s	strncpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL SSH_handle_server_ID(PTInstVar pvar, char *ID, int ID_len)

```
....
1959.                strncpy_s(prefix, sizeof(prefix), "Received server
identification string: ", _TRUNCATE);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=640

Status	New

The SSH_handle_server_ID method calls the strncpy_s function, at line 1943 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1962	1962
Object	strncpy_s	strncpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL SSH_handle_server_ID(PTInstVar pvar, char *ID, int ID_len)

```
....
1962.           strncpy_s(buf, buf_len, prefix, _TRUNCATE);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=641
Status	New

The SSH_handle_server_ID method calls the strncat_s function, at line 1943 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1963	1963
Object	strncat_s	strncat_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL SSH_handle_server_ID(PTInstVar pvar, char *ID, int ID_len)

```
....
1963.           strncat_s(buf, buf_len, ID, _TRUNCATE);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30

	062&pathid=642
Status	New

The SSH_handle_server_ID method calls the _snprintf_s function, at line 1943 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	1998	1998
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL SSH_handle_server_ID(PTInstVar pvar, char *ID, int ID_len)

```
....
1998.                              _snprintf_s(uimsg, sizeof(uimsg),
_TRUNCATE, pvar->ts->UIMsg,
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=643
Status	New

The SSH_handle_server_ID method calls the _snprintf_s function, at line 1943 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2011	2011
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL SSH_handle_server_ID(PTInstVar pvar, char *ID, int ID_len)

```
....
2011.                              _snprintf_s(TTSSH_ID, sizeof(TTSSH_ID),
_TRUNCATE,
```

Unchecked Return Value\Path 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=644
Status	New

The SSH_handle_server_ID method calls the strncpy_s function, at line 1943 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2019	2019
Object	strncpy_s	strncpy_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	BOOL SSH_handle_server_ID(PTInstVar pvar, char *ID, int ID_len)

```
....
2019.                              strncpy_s(pvar->client_version_string,
sizeof(pvar->client_version_string),
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=645
Status	New

The SSH_handle_server_ID method calls the _snprintf_s function, at line 1943 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2023	2023
Object	_snprintf_s	_snprintf_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	BOOL SSH_handle_server_ID(PTInstVar pvar, char *ID, int ID_len)

```
....
2023.                              _snprintf_s(pvar->server_version_string,
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=646
Status	New

The SSH1_handle_packet method calls the _snprintf_s function, at line 2302 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2315	2315
Object	_snprintf_s	_snprintf_s

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH1_handle_packet(PTInstVar pvar, char *data, unsigned int len, unsigned int padding)

```
....
2315.                   _snprintf_s(buf, sizeof(buf), _TRUNCATE, pvar-
>ts->UIMsg, message, handle_message_stage);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=647
Status	New

The SSH2_handle_packet method calls the _snprintf_s function, at line 2325 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2339	2339
Object	_snprintf_s	_snprintf_s

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH2_handle_packet(PTInstVar pvar, char *data, unsigned int len, unsigned int aadlen, unsigned int authlen)

```
....
2339.                   _snprintf_s(buf, sizeof(buf), _TRUNCATE, pvar-
>ts->UIMsg, message, handle_message_stage);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=648
Status	New

The SSH_get_compression_info method calls the _snprintf_s function, at line 3313 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3330	3330
Object	_snprintf_s	_snprintf_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH_get_compression_info(PTInstVar pvar, char *dest, int len)

```
....
3330.                   _snprintf_s(buf, sizeof(buf), _TRUNCATE, pvar-
>ts->UIMsg,
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=649
Status	New

The SSH_get_compression_info method calls the _snprintf_s function, at line 3313 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3336	3336
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_get_compression_info(PTInstVar pvar, char *dest, int len)

```
....
3336.                       _snprintf_s(buf, sizeof(buf), _TRUNCATE, pvar-
>ts->UIMsg,
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=650
Status	New

The SSH_get_compression_info method calls the strncpy_s function, at line 3313 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3341	3341
Object	strncpy_s	strncpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_get_compression_info(PTInstVar pvar, char *dest, int len)

```
....
3341.                 strncpy_s(buf, sizeof(buf), pvar->ts->UIMsg,
_TRUNCATE);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=651
Status	New

The SSH_get_compression_info method calls the _snprintf_s function, at line 3313 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3356	3356

Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_get_compression_info(PTInstVar pvar, char *dest, int len)

```
....
3356.                    _snprintf_s(buf2, sizeof(buf2), _TRUNCATE, pvar-
>ts->UIMsg,
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=652
Status	New

The SSH_get_compression_info method calls the _snprintf_s function, at line 3313 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3362	3362
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_get_compression_info(PTInstVar pvar, char *dest, int len)

```
....
3362.                    _snprintf_s(buf2, sizeof(buf2), _TRUNCATE, pvar-
>ts->UIMsg,
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=653
Status	New

The SSH_get_compression_info method calls the strncpy_s function, at line 3313 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-	TeraTermProject@@teraterm-teraterm-

	4_106-CVE-2023-48795-TP.c	4_106-CVE-2023-48795-TP.c
Line	3367	3367
Object	strncpy_s	strncpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_get_compression_info(PTInstVar pvar, char *dest, int len)

```
....
3367.              strncpy_s(buf2, sizeof(buf2), pvar->ts->UIMsg,
_TRUNCATE);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=654
Status	New

The SSH_get_compression_info method calls the _snprintf_s function, at line 3313 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3372	3372
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_get_compression_info(PTInstVar pvar, char *dest, int len)

```
....
3372.        _snprintf_s(dest, len, _TRUNCATE, pvar->ts->UIMsg, buf,
buf2);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=655
Status	New

The SSH_get_server_ID_info method calls the strncpy_s function, at line 3375 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3377	3377
Object	strncpy_s	strncpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_get_server_ID_info(PTInstVar pvar, char *dest, int len)

```
....
3377.       strncpy_s(dest, len,
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=656
Status	New

The SSH_get_protocol_version_info method calls the strncpy_s function, at line 3383 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3387	3387
Object	strncpy_s	strncpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_get_protocol_version_info(PTInstVar pvar, char *dest,

```
....
3387.           strncpy_s(dest, len, "Unknown", _TRUNCATE);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=657
Status	New

The SSH_get_protocol_version_info method calls the _snprintf_s function, at line 3383 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3389	3389
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_get_protocol_version_info(PTInstVar pvar, char *dest,

```
....
3389.                _snprintf_s(dest, len, _TRUNCATE, "%d.%d", pvar-
>protocol_major,
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=658
Status	New

The SSH_get_mac_info method calls the _snprintf_s function, at line 3394 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3398	3398
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH_get_mac_info(PTInstVar pvar, char *dest, int len)

```
....
3398.         _snprintf_s(dest, len, _TRUNCATE, pvar->ts->UIMsg,
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=659
Status	New

The SSH_request_X11_forwarding method calls the _snprintf_s function, at line 3897 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3916	3916
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name   TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method   void SSH_request_X11_forwarding(PTInstVar pvar,

```
....
3916.                        _snprintf_s(auth_data_ptr + i * 2,
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=660
Status	New

The SSH_request_X11_forwarding method calls the _snprintf_s function, at line 3897 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3959	3959
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name   TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method   void SSH_request_X11_forwarding(PTInstVar pvar,

```
....
3959.                        _snprintf_s(newdata + i*2, newlen - i*2,
_TRUNCATE, "%02x", auth_data[i]);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=661

Status	New

The SSH_scp_transaction method calls the strcpy_s function, at line 4103 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4134	4134
Object	strcpy_s	strcpy_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4134.                   strcpy_s(buf, sizeof(buf), "Can't open file for
reading: ");
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=662
Status	New

The SSH_scp_transaction method calls the strncpy_s function, at line 4103 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4148	4148
Object	strncpy_s	strncpy_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4148.              strncpy_s(c->scp.localfilefull, sizeof(c-
>scp.localfilefull), sendfile, _TRUNCATE);  // full path
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=663
Status	New

The SSH_scp_transaction method calls the strncpy_s function, at line 4103 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4151	4151
Object	strncpy_s	strncpy_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4151.                   strncpy_s(c->scp.remotefile, sizeof(c-
>scp.remotefile), ".", _TRUNCATE);  // full path
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=664
Status	New

The SSH_scp_transaction method calls the strncpy_s function, at line 4103 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4153	4153
Object	strncpy_s	strncpy_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4153.                    strncpy_s(c->scp.remotefile, sizeof(c-
>scp.remotefile), dstfile, _TRUNCATE);  // full path
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=665
Status	New

The SSH_scp_transaction method calls the strncpy_s function, at line 4103 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4163	4163
Object	strncpy_s	strncpy_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4163.             strncpy_s(c->scp.remotefile, sizeof(c-
>scp.remotefile), sendfile, _TRUNCATE);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=666
Status	New

The SSH_scp_transaction method calls the _snprintf_s function, at line 4103 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4174	4174
Object	_snprintf_s	_snprintf_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4174.                    _snprintf_s(c->scp.localfilefull, sizeof(c-
>scp.localfilefull), _TRUNCATE, "%s\\%s", FileDirExpanded, fn ? fn :
sendfile);
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=667
Status	New

The SSH_scp_transaction method calls the _snprintf_s function, at line 4103 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4177	4177
Object	_snprintf_s	_snprintf_s

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4177.                    _snprintf_s(c->scp.localfilefull, sizeof(c-
>scp.localfilefull), _TRUNCATE, "%s", dstfile);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=668
Status	New

The SSH_scp_transaction method calls the _snprintf_s function, at line 4103 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4185	4185
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4185.                             _snprintf_s(buf, sizeof(buf), _TRUNCATE,
"`%s' file is read only.", c->scp.localfilefull);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=669
Status	New

The SSH_scp_transaction method calls the _snprintf_s function, at line 4103 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4189	4189
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4189.                        _snprintf_s(buf, sizeof(buf), _TRUNCATE, "`%s'
file exists. (%d)\noverwrite it?", c->scp.localfilefull,
GetLastError());
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=670
Status	New

The SSH_scp_transaction method calls the strcpy_s function, at line 4103 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4200	4200
Object	strcpy_s	strcpy_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4200.                   strcpy_s(buf, sizeof(buf), "Can't open file for
writing: ");
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=671
Status	New

The debug_print method calls the _snprintf_s function, at line 4328 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4334	4334
Object	_snprintf_s	_snprintf_s

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void debug_print(int no, char *msg, int len)

```
....
4334.         _snprintf_s(file, sizeof(file), _TRUNCATE, "dump%d.bin",
no);
```

Unchecked Return Value\Path 47:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=672
Status	New

The do_write_buffer_file method calls the _snprintf_s function, at line 4352 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4357	4357
Object	_snprintf_s	_snprintf_s

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static void do_write_buffer_file(void *buf, int len, char *file, int lineno)

```
....
4357.        _snprintf_s(filename, sizeof(filename), _TRUNCATE,
"data%d.bin", lineno);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=673
Status	New

The choose_SSH2_proposal method calls the strncpy_s function, at line 4546 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4554	4554
Object	strncpy_s	strncpy_s

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void choose_SSH2_proposal(char *server_proposal,

```
....
4554.        strncpy_s(tmp_cli, sizeof(tmp_cli), my_proposal, _TRUNCATE);
```

Unchecked Return Value\Path 49:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=674
Status	New

The choose_SSH2_proposal method calls the strncpy_s function, at line 4546 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4558	4558
Object	strncpy_s	strncpy_s

Code Snippet	
File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void choose_SSH2_proposal(char *server_proposal,

```
....
4558.            strncpy_s(tmp_svr, sizeof(tmp_svr), server_proposal,
_TRUNCATE);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=675
Status	New

The choose_SSH2_proposal method calls the strncpy_s function, at line 4546 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4571	4571
Object	strncpy_s	strncpy_s

Code Snippet	
File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void choose_SSH2_proposal(char *server_proposal,

```
....
4571.            strncpy_s(dest, dest_len, ptr_cli, _TRUNCATE);
```

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=1030073&projectid=30062&pathid=918
Status	New

	Source	Destination
File	TheAlgorithms@@C-newest-CVE-2021-3520-FP.c	TheAlgorithms@@C-newest-CVE-2021-3520-FP.c
Line	227	227
Object	fgets	fgets

Code Snippet
File Name TheAlgorithms@@C-newest-CVE-2021-3520-FP.c
Method int check_placex(){

```
....
227.                fgets(input,49,stdin);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=919
Status	New

	Source	Destination
File	TheAlgorithms@@C-newest-CVE-2021-3520-FP.c	TheAlgorithms@@C-newest-CVE-2021-3520-FP.c
Line	227	227
Object	input	input

Code Snippet
File Name TheAlgorithms@@C-newest-CVE-2021-3520-FP.c
Method int check_placex(){

```
....
227.                fgets(input,49,stdin);
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=920
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8371	8371
Object	buf	buf

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static unsigned __stdcall ssh_scp_thread(void *p)

```
....
8371.               ret = fread(buf, 1, readlen, c->scp.localfp);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=921
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Line	169	169
Object	pcr_select	pcr_select

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
169.        if (fread(pcr_select, sizeof(TPML_PCR_SELECTION), 1,
pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=922
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Line	175	175
Object	Address	Address

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
175.        if (fread(&pcrs->count, sizeof(UINT32), 1, pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=923
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Line	188	188
Object	Address	Address

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
188.            if (fread(&pcrs->pcr_values[j], sizeof(TPML_DIGEST), 1,
pcr_input)
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=924
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Line	169	169
Object	pcr_select	pcr_select

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
169.       if (fread(pcr_select, sizeof(TPML_PCR_SELECTION), 1,
pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=925
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Line	175	175
Object	Address	Address

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
175.       if (fread(&pcrs->count, sizeof(UINT32), 1, pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=926
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c

Line	188	188
Object	Address	Address

Code Snippet
File Name tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
188.           if (fread(&pcrs->pcr_values[j], sizeof(TPML_DIGEST), 1,
pcr_input)
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=927
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Line	169	169
Object	pcr_select	pcr_select

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
169.       if (fread(pcr_select, sizeof(TPML_PCR_SELECTION), 1,
pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=928
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Line	175	175
Object	Address	Address

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
175.       if (fread(&pcrs->count, sizeof(UINT32), 1, pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=929
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Line	188	188
Object	Address	Address

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
188.           if (fread(&pcrs->pcr_values[j], sizeof(TPML_DIGEST), 1,
pcr_input)
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=930
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Line	169	169
Object	pcr_select	pcr_select

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
169.      if (fread(pcr_select, sizeof(TPML_PCR_SELECTION), 1,
pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=931
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Line	175	175
Object	Address	Address

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
175.      if (fread(&pcrs->count, sizeof(UINT32), 1, pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=932
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Line	188	188
Object	Address	Address

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
188.          if (fread(&pcrs->pcr_values[j], sizeof(TPML_DIGEST), 1,
pcr_input)
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=933
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Line	169	169
Object	pcr_select	pcr_select

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
169.        if (fread(pcr_select, sizeof(TPML_PCR_SELECTION), 1,
pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=934
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Line	175	175
Object	Address	Address

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
175.        if (fread(&pcrs->count, sizeof(UINT32), 1, pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=935

Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Line	188	188
Object	Address	Address

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
188.           if (fread(&pcrs->pcr_values[j], sizeof(TPML_DIGEST), 1,
pcr_input)
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=936
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Line	169	169
Object	pcr_select	pcr_select

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
169.       if (fread(pcr_select, sizeof(TPML_PCR_SELECTION), 1,
pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=937
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-	tpm2-software@@tpm2-tools-4.3.1-rc0-

	CVE-2024-29039-TP.c	CVE-2024-29039-TP.c
Line	175	175
Object	Address	Address

Code Snippet

File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c

Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
175.       if (fread(&pcrs->count, sizeof(UINT32), 1, pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=938
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Line	188	188
Object	Address	Address

Code Snippet

File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c

Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
188.           if (fread(&pcrs->pcr_values[j], sizeof(TPML_DIGEST), 1,
pcr_input)
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=939
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	237	237
Object	buffer	buffer

Code Snippet

File Name	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method	static bool parse_selection_data_from_selection_string(FILE *pcr_input,

```
....
237.                          pcrs-
>pcr_values[digest_list_count].count].buffer,
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=940
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	273	273
Object	pcr_select	pcr_select

Code Snippet

File Name	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method	static bool parse_selection_data_from_file(FILE *pcr_input,

```
....
273.       if (fread(pcr_select, sizeof(TPML_PCR_SELECTION), 1,
pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=941
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	279	279
Object	Address	Address

Code Snippet

File Name	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method	static bool parse_selection_data_from_file(FILE *pcr_input,

```
....
279.        if (fread(&pcrs->count, sizeof(UINT32), 1, pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=942
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	292	292
Object	Address	Address

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method static bool parse_selection_data_from_file(FILE *pcr_input,

```
....
292.            if (fread(&pcrs->pcr_values[j], sizeof(TPML_DIGEST), 1,
pcr_input)
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=943
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	237	237
Object	buffer	buffer

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method static bool parse_selection_data_from_selection_string(FILE *pcr_input,

```
....
237.                            pcrs-
>pcr_values[digest_list_count].count].buffer,
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=944
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	273	273
Object	pcr_select	pcr_select

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method static bool parse_selection_data_from_file(FILE *pcr_input,

```
....
273.        if (fread(pcr_select, sizeof(TPML_PCR_SELECTION), 1,
pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=945
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	279	279
Object	Address	Address

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method static bool parse_selection_data_from_file(FILE *pcr_input,

```
....
279.        if (fread(&pcrs->count, sizeof(UINT32), 1, pcr_input) != 1) {
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=946

Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	292	292
Object	Address	Address

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method static bool parse_selection_data_from_file(FILE *pcr_input,

```
....
292.          if (fread(&pcrs->pcr_values[j], sizeof(TPML_DIGEST), 1,
pcr_input)
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=947
Status	New

	Source	Destination
File	troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c	troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c
Line	367	367
Object	Address	Address

Code Snippet
File Name troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c
Method int uev_run(uev_ctx_t *ctx, int flags)

```
....
367.                          if (read(w->fd, &fdsi, sz) != sz) {
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=948
Status	New

	Source	Destination
File	troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c	troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c

Line	376	376
Object	Address	Address

Code Snippet
File Name troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c
Method int uev_run(uev_ctx_t *ctx, int flags)

```
....
376.                          if (read(w->fd, &exp, sizeof(exp)) !=
sizeof(exp)) {
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=949
Status	New

	Source	Destination
File	troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c	troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c
Line	388	388
Object	Address	Address

Code Snippet
File Name troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c
Method int uev_run(uev_ctx_t *ctx, int flags)

```
....
388.                          if (read(w->fd, &exp, sizeof(exp)) !=
sizeof(exp)) {
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=950
Status	New

	Source	Destination
File	troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c	troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c
Line	405	405
Object	Address	Address

Code Snippet

File Name	troglobit@@libuev-v2.3.1-CVE-2022-48620-TP.c
Method	int uev_run(uev_ctx_t *ctx, int flags)

```
....
405.                          if (read(w->fd, &exp, sizeof(exp)) != 
sizeof(exp))
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=951
Status	New

	Source	Destination
File	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c
Line	367	367
Object	Address	Address

Code Snippet

File Name	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c
Method	int uev_run(uev_ctx_t *ctx, int flags)

```
....
367.                          if (read(w->fd, &fdsi, sz) != sz) {
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=952
Status	New

	Source	Destination
File	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c
Line	376	376
Object	Address	Address

Code Snippet

File Name	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c
Method	int uev_run(uev_ctx_t *ctx, int flags)

```
....
376.                          if (read(w->fd, &exp, sizeof(exp)) !=
sizeof(exp)) {
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=953
Status	New

	Source	Destination
File	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c
Line	388	388
Object	Address	Address

Code Snippet

File Name	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c
Method	int uev_run(uev_ctx_t *ctx, int flags)

```
....
388.                          if (read(w->fd, &exp, sizeof(exp)) !=
sizeof(exp)) {
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=954
Status	New

	Source	Destination
File	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c
Line	405	405
Object	Address	Address

Code Snippet

File Name	troglobit@@libuev-v2.3.2-CVE-2022-48620-TP.c
Method	int uev_run(uev_ctx_t *ctx, int flags)

```
....
405.                          if (read(w->fd, &exp, sizeof(exp)) !=
sizeof(exp))
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=955
Status	New

	Source	Destination
File	troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c	troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c
Line	373	373
Object	Address	Address

Code Snippet
File Name troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c
Method int uev_run(uev_ctx_t *ctx, int flags)

```
....
373.                              if (read(w->fd, &fdsi, sz) != sz) {
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=956
Status	New

	Source	Destination
File	troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c	troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c
Line	384	384
Object	Address	Address

Code Snippet
File Name troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c
Method int uev_run(uev_ctx_t *ctx, int flags)

```
....
384.                              if (read(w->fd, &exp, sizeof(exp)) !=
sizeof(exp)) {
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30

	062&pathid=957
Status	New

	Source	Destination
File	troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c	troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c
Line	396	396
Object	Address	Address

Code Snippet
File Name troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c
Method int uev_run(uev_ctx_t *ctx, int flags)

```
....
396.                              if (read(w->fd, &exp, sizeof(exp)) !=
sizeof(exp)) {
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=958
Status	New

	Source	Destination
File	troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c	troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c
Line	413	413
Object	Address	Address

Code Snippet
File Name troglobit@@libuev-v2.4.0-CVE-2022-48620-TP.c
Method int uev_run(uev_ctx_t *ctx, int flags)

```
....
413.                              if (read(w->fd, &exp, sizeof(exp)) !=
sizeof(exp))
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=959
Status	New

	Source	Destination

File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	474	474
Object	fprintf	fprintf

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void displine_memdump(FILE *fp, int addr, int *bytes, int byte_cnt)

```
....
474.         fprintf(fp, "%08X : ", addr);
```

Improper Resource Access Authorization\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=960
Status New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	479	479
Object	fprintf	fprintf

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void displine_memdump(FILE *fp, int addr, int *bytes, int byte_cnt)

```
....
479.                     fprintf(fp, " ");
```

Improper Resource Access Authorization\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=961
Status New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	481	481
Object	fprintf	fprintf

Code Snippet	
File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void displine_memdump(FILE *fp, int addr, int *bytes, int byte_cnt)

```
....
481.                fprintf(fp, "%02X", bytes[i]);
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=962
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	485	485
Object	fprintf	fprintf

Code Snippet	
File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void displine_memdump(FILE *fp, int addr, int *bytes, int byte_cnt)

```
....
485.          fprintf(fp, "    %*s%*s", (16-byte_cnt)*2+1, " ", (16-
byte_cnt+3)/4, " ");
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=963
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	491	491
Object	fprintf	fprintf

Code Snippet	
File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void displine_memdump(FILE *fp, int addr, int *bytes, int byte_cnt)

```
....
491.                        fprintf(fp, "%c", c);
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=964
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	493	493
Object	fprintf	fprintf

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void displine_memdump(FILE *fp, int addr, int *bytes, int byte_cnt)

```
....
493.                        fprintf(fp, ".");
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=965
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	497	497
Object	fprintf	fprintf

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void displine_memdump(FILE *fp, int addr, int *bytes, int byte_cnt)

```
....
497.            fprintf(fp, "\n");
```

Improper Resource Access Authorization\Path 49:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=966
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	579	579
Object	fprintf	fprintf

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void save_memdump(char *filename)

```
....
579.         fprintf(fp, "<<< Tera Term SSH2 log dump >>>\n");
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=967
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	580	580
Object	fprintf	fprintf

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void save_memdump(char *filename)

```
....
580.         fprintf(fp, "saved time: %04d/%02d/%02d %02d:%02d:%02d\n",
```

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=1030073&projectid=30062&pathid=801
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 2148 is not initialized when it is used by self_id at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2161	3579
Object	null	self_id

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static BOOL handle_channel_data(PTInstVar pvar)

```
....
2161.                    SSH_agent_response(pvar, NULL,
local_channel_num,
```

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3579.                            "local:%d remote:%d len:%d",
__FUNCTION__, c->self_id, c->remote_id, buflen);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=802
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by self_id at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Line	3538	3579
Object	null	self_id

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.             c = NULL;
....
3579.                          "local:%d remote:%d len:%d",
__FUNCTION__, c->self_id, c->remote_id, buflen);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=803
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 2148 is not initialized when it is used by remote_id at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2161	3568
Object	null	remote_id

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_channel_data(PTInstVar pvar)

```
....
2161.                   SSH_agent_response(pvar, NULL,
local_channel_num,
```

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3568.             buffer_put_int(msg, c->remote_id);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=804
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by remote_id at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	3568
Object	null	remote_id

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.                   c = NULL;
....
3568.                   buffer_put_int(msg, c->remote_id);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=805
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 2148 is not initialized when it is used by remote_id at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2161	3579
Object	null	remote_id

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_channel_data(PTInstVar pvar)

```
....
2161.                   SSH_agent_response(pvar, NULL,
local_channel_num,
```

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3579.                            "local:%d remote:%d len:%d",
__FUNCTION__, c->self_id, c->remote_id, buflen);
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=806
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by remote_id at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	3579
Object	null	remote_id

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.             c = NULL;
....
3579.                            "local:%d remote:%d len:%d",
__FUNCTION__, c->self_id, c->remote_id, buflen);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=807
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 2148 is not initialized when it is used by bufchain at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 241.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2161	257
Object	null	bufchain

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static BOOL handle_channel_data(PTInstVar pvar)

```
....
2161.                   SSH_agent_response(pvar, NULL,
local_channel_num,
```

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static void ssh2_channel_add_bufchain(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen)

```
....
257.          if (c->bufchain == NULL) {
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=808
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by bufchain at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 241.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	257
Object	null	bufchain

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.                   c = NULL;
```

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void ssh2_channel_add_bufchain(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen)

```
....
257.            if (c->bufchain == NULL) {
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=809
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 2148 is not initialized when it is used by bufchain_amount at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 241.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	2161	267
Object	null	bufchain_amount

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static BOOL handle_channel_data(PTInstVar pvar)

```
....
2161.                   SSH_agent_response(pvar, NULL,
local_channel_num,
```

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void ssh2_channel_add_bufchain(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen)

```
....
267.            c->bufchain_amount += buflen;
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=810
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by bufchain_amount at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 241.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	267
Object	null	bufchain_amount

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.               c = NULL;
```

▼

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static void ssh2_channel_add_bufchain(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen)

```
....
267.         c->bufchain_amount += buflen;
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=811
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by bufchain_amount at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 276.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	301
Object	null	bufchain_amount

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.                  c = NULL;
```

▼

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static void ssh2_channel_retry_send_bufchain(PTInstVar pvar, Channel_t *c)

```
....
301.                   c->bufchain_amount -= size;
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=812
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by local_window_max at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 8152.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	8173
Object	null	local_window_max

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.                  c = NULL;
```

▼

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static void do_SSH2_adjust_window_size(PTInstVar pvar, Channel_t *c)

```
....
8173.                  buffer_put_int(msg, c->local_window_max - c-
>local_window);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=813
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by local_window at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 8152.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	8173
Object	null	local_window

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.           c = NULL;
```

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void do_SSH2_adjust_window_size(PTInstVar pvar, Channel_t *c)

```
....
8173.           buffer_put_int(msg, c->local_window_max - c-
>local_window);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=814
Status	New

The variable declared in null at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 3526 is not initialized when it is used by remote_id at TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c in line 8152.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	3538	8172

Object	null	remote_id

Code Snippet

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method void SSH2_send_channel_data(PTInstVar pvar, Channel_t *c, unsigned char *buf, unsigned int buflen, int retry)

```
....
3538.                c = NULL;
```

File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method static void do_SSH2_adjust_window_size(PTInstVar pvar, Channel_t *c)

```
....
8172.                buffer_put_int(msg, c->remote_id);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=815
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c in line 169 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c in line 198.

	Source	Destination
File	TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c
Line	194	234
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c

Method Statement::BindParameter(const Local<Value> source, T pos) {

```
....
194.             return NULL;
```

File Name TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c

Method template <class T> T* Statement::Bind(Nan::NAN_METHOD_ARGS_TYPE info, int start, int last) {

```
....
234.                          baton->parameters.push_back(
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=816
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c in line 169 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c in line 198.

	Source	Destination
File	TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c
Line	194	238
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c

Method Statement::BindParameter(const Local<Value> source, T pos) {

```
....
194.              return NULL;
```

File Name TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c

Method template <class T> T* Statement::Bind(Nan::NAN_METHOD_ARGS_TYPE info, int start, int last) {

```
....
238.                          baton-
>parameters.push_back(BindParameter(Nan::Get(object,
name).ToLocalChecked(),
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=817
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c in line 169 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c in line 198.

	Source	Destination
File	TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c
Line	194	223
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c
Method Statement::BindParameter(const Local<Value> source, T pos) {

```
....
194.            return NULL;
```

File Name TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c
Method template <class T> T* Statement::Bind(Nan::NAN_METHOD_ARGS_TYPE info, int start, int last) {

```
....
223.                    baton->parameters.push_back(BindParameter(info[i],
pos));
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=818
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c in line 169 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c in line 198.

	Source	Destination
File	TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c
Line	194	216
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c
Method Statement::BindParameter(const Local<Value> source, T pos) {

```
....
194.            return NULL;
```

File Name	TryGhost@@node-sqlite3-v4.2.0-CVE-2022-21227-TP.c
Method	template <class T> T* Statement::Bind(Nan::NAN_METHOD_ARGS_TYPE info, int start, int last) {

```
....
216.                      baton-
>parameters.push_back(BindParameter(Nan::Get(array, i).ToLocalChecked(),
pos));
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=819
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c in line 216.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Line	212	254
Object	null	parameters

Code Snippet

File Name	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Method	Statement::BindParameter(const Napi::Value source, T pos) {

```
....
212.           return NULL;
```

▾

File Name	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
254.                          baton->parameters.push_back(
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=820
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c in line 216.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Line	212	258
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
212.            return NULL;
```

File Name TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
258.                            baton-
>parameters.push_back(BindParameter((object).Get(name),
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=821
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c in line 216.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Line	212	242
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
212.          return NULL;
```

File Name	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
242.                  baton->parameters.push_back(BindParameter(info[i],
pos));
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=822
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c in line 216.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Line	212	235
Object	null	parameters

Code Snippet

File Name	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Method	Statement::BindParameter(const Napi::Value source, T pos) {

```
....
212.          return NULL;
```

File Name	TryGhost@@node-sqlite3-v5.0.1-CVE-2022-21227-TP.c
Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
235.                  baton-
>parameters.push_back(BindParameter((array).Get(i), pos));
```

NULL Pointer Dereference\Path 23:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=823
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c in line 216.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c
Line	212	254
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c

Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
212.            return NULL;
```

File Name TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
254.                        baton->parameters.push_back(
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=824
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c in line 216.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c
Line	212	258
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
212.            return NULL;
```

▼

File Name TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c
Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
258.                        baton-
>parameters.push_back(BindParameter((object).Get(name),
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=825
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c in line 216.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c
Line	212	242
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
212.            return NULL;
```

▼

File Name TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c
Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
242.                  baton->parameters.push_back(BindParameter(info[i],
pos));
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=826
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c in line 216.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c	TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c
Line	212	235
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c

Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
212.          return NULL;
```

File Name TryGhost@@node-sqlite3-v5.0.2-CVE-2022-21227-TP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
235.                    baton-
>parameters.push_back(BindParameter((array).Get(i), pos));
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=827
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c

Line	211	260
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c

Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
211.                return NULL;
```

▼

File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
260.                        baton->parameters.push_back(
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=828
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Line	218	260
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c

Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
218.            return NULL;
```

▼

File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
260.                          baton->parameters.push_back(
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=829
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Line	211	264
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c

Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
211.                  return NULL;
```

File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
264.                          baton-
>parameters.push_back(BindParameter((object).Get(name),
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=830
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Line	218	264
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
218.            return NULL;
```

File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
264.                          baton-
>parameters.push_back(BindParameter((object).Get(name),
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=831
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Line	211	248
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
211.                return NULL;
```

File Name	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
248.                    baton->parameters.push_back(BindParameter(info[i],
pos));
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=832
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Line	218	248
Object	null	parameters

Code Snippet

File Name	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Method	Statement::BindParameter(const Napi::Value source, T pos) {

```
....
218.            return NULL;
```

File Name	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
248.                    baton->parameters.push_back(BindParameter(info[i],
pos));
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=833
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Line	211	241
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
211.                return NULL;
```

File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
241.                    baton-
>parameters.push_back(BindParameter((array).Get(i), pos));
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=834
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Line	218	241
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
218.            return NULL;
```

▼

File Name TryGhost@@node-sqlite3-v5.0.3-CVE-2022-21227-FP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
241.                    baton-
>parameters.push_back(BindParameter((array).Get(i), pos));
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=835
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Line	211	260
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c

Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
211.                return NULL;
```

▼

File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
260.                        baton->parameters.push_back(
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=836
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Line	218	260
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c

Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
218.            return NULL;
```

File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
260.                        baton->parameters.push_back(
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=837
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Line	211	264
Object	null	parameters

Code Snippet

File Name	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Method	Statement::BindParameter(const Napi::Value source, T pos) {

```
....
211.                return NULL;
```

File Name	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
264.                            baton-
>parameters.push_back(BindParameter((object).Get(name),
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=838
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Line	218	264
Object	null	parameters

Code Snippet

File Name	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Method	Statement::BindParameter(const Napi::Value source, T pos) {

```
....
218.            return NULL;
```

File Name	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
264.                            baton-
>parameters.push_back(BindParameter((object).Get(name),
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=839
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Line	211	248
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c

Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
211.                return NULL;
```

▼

File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
248.                     baton->parameters.push_back(BindParameter(info[i], 
pos));
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=840
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Line	218	248

Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
218.            return NULL;
```

File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
248.                    baton->parameters.push_back(BindParameter(info[i],
pos));
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=841
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Line	211	241
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
211.                return NULL;
```

File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
241.                      baton-
>parameters.push_back(BindParameter((array).Get(i), pos));
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=842
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 178 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c in line 222.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Line	218	241
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
218.          return NULL;
```

File Name TryGhost@@node-sqlite3-v5.0.9-CVE-2022-21227-FP.c
Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
241.                      baton-
>parameters.push_back(BindParameter((array).Get(i), pos));
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=843
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 181 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 225.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Line	214	263
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
214.                return NULL;
```

▼

File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
263.                        baton->parameters.push_back(
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=844
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 181 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 225.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Line	221	263
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
221.            return NULL;
```

▼

File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c

Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
263.                            baton->parameters.push_back(
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=845
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 181 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 225.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Line	214	267
Object	null	parameters

Code Snippet

File Name	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method	Statement::BindParameter(const Napi::Value source, T pos) {

```
....
214.                  return NULL;
```

File Name	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
267.                            baton-
>parameters.push_back(BindParameter((object).Get(name),
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=846
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 181 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 225.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Line	221	267
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
221.            return NULL;
```

File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
267.                        baton-
>parameters.push_back(BindParameter((object).Get(name),
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=847
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 181 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 225.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Line	214	251
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
214.                return NULL;
```

File Name	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
251.                    baton->parameters.push_back(BindParameter(info[i],
pos));
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=848
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 181 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 225.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Line	221	251
Object	null	parameters

Code Snippet

File Name	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method	Statement::BindParameter(const Napi::Value source, T pos) {

```
....
221.            return NULL;
```

File Name	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method	template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
251.                    baton->parameters.push_back(BindParameter(info[i],
pos));
```

NULL Pointer Dereference\Path 49:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=849
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 181 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 225.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Line	214	244
Object	null	parameters

Code Snippet

File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c

Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
214.                return NULL;
```

File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
244.                    baton-
>parameters.push_back(BindParameter((array).Get(i), pos));
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=850
Status	New

The variable declared in null at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 181 is not initialized when it is used by parameters at TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c in line 225.

	Source	Destination
File	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c	TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Line	221	244
Object	null	parameters

Code Snippet
File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c
Method Statement::BindParameter(const Napi::Value source, T pos) {

```
....
221.            return NULL;
```

File Name TryGhost@@node-sqlite3-v5.1.3-CVE-2022-21227-FP.c

Method template <class T> T* Statement::Bind(const Napi::CallbackInfo& info, int start, int last) {

```
....
244.                      baton-
>parameters.push_back(BindParameter((array).Get(i), pos));
```

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=1030073&projectid=30062&pathid=1043
Status	New

The save_memdump method in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	572	572
Object	fopen	fopen

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void save_memdump(char *filename)

```
....
572.        fp = fopen(filename, "w");
```

TOCTOU\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1044
Status	New

The SSH_scp_transaction method in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4130	4130
Object	fopen	fopen

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4130.               fp = fopen(sendfile, "rb");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1045
Status	New

The SSH_scp_transaction method in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4196	4196
Object	fopen	fopen

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4196.               fp = fopen(c->scp.localfilefull, "wb");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1046
Status	New

The debug_print method in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4336	4336
Object	fopen	fopen

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void debug_print(int no, char *msg, int len)

```
....
4336.        fp = fopen(file, "wb");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1047
Status	New

The do_write_buffer_file method in TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-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	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4359	4359
Object	fopen	fopen

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static void do_write_buffer_file(void *buf, int len, char *file, int lineno)

```
....
4359.        fp = fopen(filename, "wb");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1048
Status	New

The CSecurityTLS::checkSession method in TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-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	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Line	436	436
Object	fopen	fopen

Code Snippet
File Name TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Method void CSecurityTLS::checkSession()

```
....
436.       f = fopen(caSave.buf, "a+");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1049
Status	New

The verify_signature method in tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-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	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Line	56	56
Object	fopen	fopen

Code Snippet
File Name tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Method static bool verify_signature() {

```
....
56.       FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1050
Status	New

The pcrs_from_file method in tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-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	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Line	161	161
Object	fopen	fopen

Code Snippet
File Name tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.      FILE *pcr_input = fopen(pcr_file_path, "rb");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1051
Status	New

The verify_signature method in tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-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	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Line	56	56
Object	fopen	fopen

Code Snippet
File Name tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Method static bool verify_signature() {

```
....
56.       FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1052
Status	New

The pcrs_from_file method in tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-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	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Line	161	161
Object	fopen	fopen

Code Snippet
File Name tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.       FILE *pcr_input = fopen(pcr_file_path, "rb");
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1053
Status	New

The verify_signature method in tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-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	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Line	56	56
Object	fopen	fopen

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c

Method static bool verify_signature() {

```
....
56.       FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1054
Status	New

The pcrs_from_file method in tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-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	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Line	161	161
Object	fopen	fopen

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.      FILE *pcr_input = fopen(pcr_file_path, "rb");
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1055
Status	New

The verify_signature method in tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-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	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Line	56	56
Object	fopen	fopen

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Method	static bool verify_signature() {

```
....
56.       FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1056
Status	New

The pcrs_from_file method in tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-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	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Line	161	161
Object	fopen	fopen

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.       FILE *pcr_input = fopen(pcr_file_path, "rb");
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1057
Status	New

The verify_signature method in tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-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	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Line	56	56
Object	fopen	fopen

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Method static bool verify_signature() {

```
....
56.      FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1058
Status	New

The pcrs_from_file method in tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-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	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Line	161	161
Object	fopen	fopen

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.      FILE *pcr_input = fopen(pcr_file_path, "rb");
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1059
Status	New

The verify_signature method in tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-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	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Line	56	56
Object	fopen	fopen

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Method	static bool verify_signature() {

```
....
56.       FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1060
Status	New

The pcrs_from_file method in tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-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	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Line	161	161
Object	fopen	fopen

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.       FILE *pcr_input = fopen(pcr_file_path, "rb");
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1061
Status	New

The pcrs_from_file method in tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-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	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	317	317

Object	fopen	fopen

Code Snippet

File Name	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
317.        FILE *pcr_input = fopen(pcr_file_path, "rb");
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1062
Status	New

The pcrs_from_file method in tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-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	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	317	317
Object	fopen	fopen

Code Snippet

File Name	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
317.        FILE *pcr_input = fopen(pcr_file_path, "rb");
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1063
Status	New

The fuse_mount_fusermount method in tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-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	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c

Line	450	450
Object	open	open

Code Snippet
File Name tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method static int fuse_mount_fusermount(const char *mountpoint, const char *opts,

```
....
450.                    int fd = open("/dev/null", O_RDONLY);
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1064
Status	New

The fuse_mount_sys method in tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-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	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Line	510	510
Object	open	open

Code Snippet
File Name tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method static int fuse_mount_sys(const char *mnt, struct mount_opts *mo,

```
....
510.         fd = open(devname, O_RDWR);
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1065
Status	New

The fuse_mount_fusermount method in tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-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	tuxera@@ntfs-3g-2021.8.22-CVE-2022-	tuxera@@ntfs-3g-2021.8.22-CVE-2022-

	30783-TP.c	30783-TP.c
Line	450	450
Object	open	open

Code Snippet
File Name tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method static int fuse_mount_fusermount(const char *mountpoint, const char *opts,

```
....
450.                    int fd = open("/dev/null", O_RDONLY);
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1066
Status	New

The fuse_mount_sys method in tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-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	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Line	510	510
Object	open	open

Code Snippet
File Name tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method static int fuse_mount_sys(const char *mnt, struct mount_opts *mo,

```
....
510.        fd = open(devname, O_RDWR);
```

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=1030073&projectid=30062&pathid=1009
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	572	572
Object	fp	fp

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void save_memdump(char *filename)

```
....
572.          fp = fopen(filename, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1010
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4130	4130
Object	fp	fp

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4130.               fp = fopen(sendfile, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1011
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4196	4196
Object	fp	fp

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method int SSH_scp_transaction(PTInstVar pvar, char *sendfile, char *dstfile, enum scp_dir direction)

```
....
4196.                fp = fopen(c->scp.localfilefull, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1012
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4336	4336
Object	fp	fp

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method void debug_print(int no, char *msg, int len)

```
....
4336.        fp = fopen(file, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1013
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4359	4359

Object	fp	fp

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static void do_write_buffer_file(void *buf, int len, char *file, int lineno)

```
....
4359.        fp = fopen(filename, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1014
Status	New

	Source	Destination
File	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Line	436	436
Object	f	f

Code Snippet
File Name TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Method void CSecurityTLS::checkSession()

```
....
436.        f = fopen(caSave.buf, "a+");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1015
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Line	56	56
Object	pubkey_input	pubkey_input

Code Snippet
File Name tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Method static bool verify_signature() {

```
....
56.       FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1016
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Line	161	161
Object	pcr_input	pcr_input

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29038-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.      FILE *pcr_input = fopen(pcr_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1017
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Line	56	56
Object	pubkey_input	pubkey_input

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Method	static bool verify_signature() {

```
....
56.       FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1018
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Line	161	161
Object	pcr_input	pcr_input

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.1.2-rc0-CVE-2024-29039-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.        FILE *pcr_input = fopen(pcr_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1019
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Line	56	56
Object	pubkey_input	pubkey_input

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Method	static bool verify_signature() {

```
....
56.        FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1020
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Line	161	161
Object	pcr_input	pcr_input

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29038-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.        FILE *pcr_input = fopen(pcr_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1021
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Line	56	56
Object	pubkey_input	pubkey_input

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Method static bool verify_signature() {

```
....
56.       FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1022
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Line	161	161

Object	pcr_input	pcr_input

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.0-rc0-CVE-2024-29039-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.        FILE *pcr_input = fopen(pcr_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1023
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Line	56	56
Object	pubkey_input	pubkey_input

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Method static bool verify_signature() {

```
....
56.         FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1024
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Line	161	161
Object	pcr_input	pcr_input

Code Snippet
File Name tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29038-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.        FILE *pcr_input = fopen(pcr_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1025
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Line	56	56
Object	pubkey_input	pubkey_input

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Method	static bool verify_signature() {

```
....
56.        FILE *pubkey_input = fopen(ctx.pubkey_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1026
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Line	161	161
Object	pcr_input	pcr_input

Code Snippet

File Name	tpm2-software@@tpm2-tools-4.3.1-rc0-CVE-2024-29039-TP.c
Method	static bool pcrs_from_file(const char *pcr_file_path,

```
....
161.        FILE *pcr_input = fopen(pcr_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1027
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Line	317	317
Object	pcr_input	pcr_input

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29038-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
317.       FILE *pcr_input = fopen(pcr_file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=1028
Status	New

	Source	Destination
File	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c	tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Line	317	317
Object	pcr_input	pcr_input

Code Snippet
File Name tpm2-software@@tpm2-tools-5.6.1-rc0-CVE-2024-29039-TP.c
Method static bool pcrs_from_file(const char *pcr_file_path,

```
....
317.       FILE *pcr_input = fopen(pcr_file_path, "rb");
```

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=1030073&projectid=30062&pathid=1029
Status	New

The system data read by receive_fd in the file tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 321 is potentially exposed by receive_fd found in tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 321.

	Source	Destination
File	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Line	344	344
Object	perror	perror

Code Snippet
File Name tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method static int receive_fd(int fd)

```
....
344.            perror("recvmsg");
```

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=1030073&projectid=30062&pathid=1030
Status	New

The system data read by fuse_mount_fusermount in the file tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 418 is potentially exposed by fuse_mount_fusermount found in tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 418.

	Source	Destination
File	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Line	432	432
Object	perror	perror

Code Snippet
File Name tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method static int fuse_mount_fusermount(const char *mountpoint, const char *opts,

```
....
432.            perror("fuse: socketpair() failed");
```

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=1030073&projectid=30062&pathid=1031
Status	New

The system data read by fuse_mount_fusermount in the file tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 418 is potentially exposed by fuse_mount_fusermount found in tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 418.

	Source	Destination
File	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Line	438	438
Object	perror	perror

Code Snippet
File Name tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method static int fuse_mount_fusermount(const char *mountpoint, const char *opts,

```
....
438.            perror("fuse: fork() failed");
```

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=1030073&projectid=30062&pathid=1032
Status	New

The system data read by fuse_mount_fusermount in the file tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 418 is potentially exposed by fuse_mount_fusermount found in tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 418.

	Source	Destination
File	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Line	469	469
Object	perror	perror

Code Snippet
File Name tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method static int fuse_mount_fusermount(const char *mountpoint, const char *opts,

```
....
469.            perror("fuse: failed to exec fusermount");
```

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=1030073&projectid=30062&pathid=1033
Status	New

The system data read by receive_fd in the file tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 321 is potentially exposed by receive_fd found in tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 321.

	Source	Destination
File	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Line	344	344
Object	perror	perror

Code Snippet

File Name	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method	static int receive_fd(int fd)

```
....
344.          perror("recvmsg");
```

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=1030073&projectid=30062&pathid=1034
Status	New

The system data read by fuse_mount_fusermount in the file tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 418 is potentially exposed by fuse_mount_fusermount found in tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 418.

	Source	Destination
File	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Line	432	432
Object	perror	perror

Code Snippet

File Name	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method	static int fuse_mount_fusermount(const char *mountpoint, const char *opts,

```
....
432.          perror("fuse: socketpair() failed");
```

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=1030073&projectid=30062&pathid=1035
Status	New

The system data read by fuse_mount_fusermount in the file tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 418 is potentially exposed by fuse_mount_fusermount found in tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 418.

	Source	Destination
File	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Line	438	438
Object	perror	perror

Code Snippet

File Name	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method	static int fuse_mount_fusermount(const char *mountpoint, const char *opts,

```
....
438.            perror("fuse: fork() failed");
```

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=1030073&projectid=30062&pathid=1036
Status	New

The system data read by fuse_mount_fusermount in the file tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 418 is potentially exposed by fuse_mount_fusermount found in tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 418.

	Source	Destination
File	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Line	469	469
Object	perror	perror

Code Snippet

File Name	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method	static int fuse_mount_fusermount(const char *mountpoint, const char *opts,

```
....
469.          perror("fuse: failed to exec fusermount");
```

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=1030073&projectid=30062&pathid=1037
Status	New

The system data read by fuse_mount_sys in the file tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 481 is potentially exposed by fuse_mount_sys found in tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 481.

	Source	Destination
File	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Line	500	499
Object	errno	fprintf

Code Snippet
File Name tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method static int fuse_mount_sys(const char *mnt, struct mount_opts *mo,

```
....
500.                    mnt, strerror(errno));
....
499.          fprintf(stderr ,"fuse: failed to access mountpoint %s:
%s\n",
```

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=1030073&projectid=30062&pathid=1038
Status	New

The system data read by fuse_mount_sys in the file tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 481 is potentially exposed by fuse_mount_sys found in tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 481.

	Source	Destination
File	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Line	517	516
Object	errno	fprintf

Code Snippet	
File Name	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method	static int fuse_mount_sys(const char *mnt, struct mount_opts *mo,

```
....
517.                    strerror(errno));
....
516.                fprintf(stderr, "fuse: failed to open %s: %s\n",
devname,
```

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=1030073&projectid=30062&pathid=1039
Status	New

The system data read by fuse_mount_sys in the file tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 481 is potentially exposed by fuse_mount_sys found in tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c at line 481.

	Source	Destination
File	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Line	571	575
Object	errno	fprintf

Code Snippet	
File Name	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method	static int fuse_mount_sys(const char *mnt, struct mount_opts *mo,

```
....
571.                int errno_save = errno;
....
575.                    fprintf(stderr, "fuse: mount failed: %s\n",
```

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=1030073&projectid=30062&pathid=1040
Status	New

The system data read by fuse_mount_sys in the file tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 481 is potentially exposed by fuse_mount_sys found in tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 481.

	Source	Destination
File	tuxera@@ntfs-3g-2021.8.22-CVE-2022-	tuxera@@ntfs-3g-2021.8.22-CVE-2022-

	30783-TP.c	30783-TP.c
Line	500	499
Object	errno	fprintf

Code Snippet
File Name tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method static int fuse_mount_sys(const char *mnt, struct mount_opts *mo,

```
....
500.                      mnt, strerror(errno));
....
499.             fprintf(stderr ,"fuse: failed to access mountpoint %s: 
%s\n",
```

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=1030073&projectid=30062&pathid=1041
Status	New

The system data read by fuse_mount_sys in the file tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 481 is potentially exposed by fuse_mount_sys found in tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 481.

	Source	Destination
File	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Line	517	516
Object	errno	fprintf

Code Snippet
File Name tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method static int fuse_mount_sys(const char *mnt, struct mount_opts *mo,

```
....
517.                          strerror(errno));
....
516.                 fprintf(stderr, "fuse: failed to open %s: %s\n", 
devname,
```

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=1030073&projectid=30062&pathid=1042
Status	New

The system data read by fuse_mount_sys in the file tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 481 is potentially exposed by fuse_mount_sys found in tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c at line 481.

	Source	Destination
File	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Line	571	575
Object	errno	fprintf

Code Snippet
File Name tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method static int fuse_mount_sys(const char *mnt, struct mount_opts *mo,

```
....
571.                int errno_save = errno;
....
575.                    fprintf(stderr, "fuse: mount failed: %s\n",
```

Potential Precision Problem

Query Path:
CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Precision Problem\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=886
Status	New

The size of the buffer used by SSH2_scp_fromremote in "C%o %lld %s", at line 8707 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SSH2_scp_fromremote passes to "C%o %lld %s", at line 8707 of TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c, to overwrite the target buffer.

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8741	8741
Object	"C%o %lld %s"	"C%o %lld %s"

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c

Method	static BOOL SSH2_scp_fromremote(PTInstVar pvar, Channel_t *c, unsigned char *data, unsigned int buflen)

```
....
8741.                    sscanf_s(data, "C%o %lld %s", &permission,
&size, filename, (unsigned int)sizeof(filename));
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=887
Status	New

The size of the buffer used by CSecurityTLS::checkSession in "%sx509_savedcerts.pem", at line 284 of TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CSecurityTLS::checkSession passes to "%sx509_savedcerts.pem", at line 284 of TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c, to overwrite the target buffer.

	Source	Destination
File	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Line	434	434
Object	"%sx509_savedcerts.pem"	"%sx509_savedcerts.pem"

Code Snippet

File Name	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Method	void CSecurityTLS::checkSession()

```
....
434.      sprintf(caSave.buf, "%sx509_savedcerts.pem", homeDir);
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=888
Status	New

The size of the buffer used by CSecurityTLS::setDefaults in "%sx509_ca.pem", at line 80 of TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CSecurityTLS::setDefaults passes to "%sx509_ca.pem", at line 80 of TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c, to overwrite the target buffer.

	Source	Destination
File	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Line	92	92

Object	"%sx509_ca.pem"	"%sx509_ca.pem"

Code Snippet
File Name TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Method void CSecurityTLS::setDefaults()

```
....
92.     sprintf(caDefault.buf, "%sx509_ca.pem", homeDir);
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=889
Status	New

The size of the buffer used by CSecurityTLS::setDefaults in "%s509_crl.pem", at line 80 of TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CSecurityTLS::setDefaults passes to "%s509_crl.pem", at line 80 of TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c, to overwrite the target buffer.

	Source	Destination
File	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Line	93	93
Object	"%s509_crl.pem"	"%s509_crl.pem"

Code Snippet
File Name TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Method void CSecurityTLS::setDefaults()

```
....
93.     sprintf(crlDefault.buf, "%s509_crl.pem", homeDir);
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=890
Status	New

The size of the buffer used by CSecurityTLS::setParam in "%sx509_savedcerts.pem", at line 208 of TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CSecurityTLS::setParam passes to "%sx509_savedcerts.pem", at line 208 of TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c, to overwrite the target buffer.

	Source	Destination

File	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c	TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Line	260	260
Object	"%sx509_savedcerts.pem"	"%sx509_savedcerts.pem"

Code Snippet
File Name TigerVNC@@tigervnc-v1.10.90-CVE-2020-26117-TP.c
Method void CSecurityTLS::setParam()

```
....
260.         sprintf(caSave.buf, "%sx509_savedcerts.pem", homeDir);
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=891
Status	New

The size of the buffer used by CSecurityTLS::checkSession in "%sx509_known_hosts", at line 308 of TigerVNC@@tigervnc-v1.11.90-CVE-2020-26117-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CSecurityTLS::checkSession passes to "%sx509_known_hosts", at line 308 of TigerVNC@@tigervnc-v1.11.90-CVE-2020-26117-TP.c, to overwrite the target buffer.

	Source	Destination
File	TigerVNC@@tigervnc-v1.11.90-CVE-2020-26117-TP.c	TigerVNC@@tigervnc-v1.11.90-CVE-2020-26117-TP.c
Line	403	403
Object	"%sx509_known_hosts"	"%sx509_known_hosts"

Code Snippet
File Name TigerVNC@@tigervnc-v1.11.90-CVE-2020-26117-TP.c
Method void CSecurityTLS::checkSession()

```
....
403.     sprintf(dbPath.buf, "%sx509_known_hosts", homeDir);
```

Potential Precision Problem\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=892
Status	New

The size of the buffer used by fuse_mount_sys in "%s#%s", at line 481 of tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fuse_mount_sys passes to "%s#%s", at line 481 of tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c, to overwrite the target buffer.

	Source	Destination
File	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Line	555	555
Object	"%s#%s"	"%s#%s"

Code Snippet
File Name tuxera@@ntfs-3g-2021.5.19-CVE-2022-30783-TP.c
Method static int fuse_mount_sys(const char *mnt, struct mount_opts *mo,

```
....
555.                  sprintf(source, "%s#%s", mo->subtype, mo->fsname);
```

Potential Precision Problem\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=893
Status	New

The size of the buffer used by fuse_mount_sys in "%s#%s", at line 481 of tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fuse_mount_sys passes to "%s#%s", at line 481 of tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c, to overwrite the target buffer.

	Source	Destination
File	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c	tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Line	555	555
Object	"%s#%s"	"%s#%s"

Code Snippet
File Name tuxera@@ntfs-3g-2021.8.22-CVE-2022-30783-TP.c
Method static int fuse_mount_sys(const char *mnt, struct mount_opts *mo,

```
....
555.                  sprintf(source, "%s#%s", mo->subtype, mo->fsname);
```

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=1030073&projectid=30

	062&pathid=792
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5537	5543
Object	hostkey	sizeof

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static BOOL handle_SSH2_dh_kex_reply(PTInstVar pvar)

```
....
5537.        Key *hostkey = NULL;  // hostkey
....
5543.        memset(&hostkey, 0, sizeof(hostkey));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=793
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5645	5651
Object	hostkey	sizeof

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	BOOL handle_SSH2_dh_kex_reply_after_known_hosts(PTInstVar pvar)

```
....
5645.        Key *hostkey = NULL;  // hostkey
....
5651.        memset(&hostkey, 0, sizeof(hostkey));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=794
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5802	5808
Object	hostkey	sizeof

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_dh_gex_reply(PTInstVar pvar)

```
....
5802.       Key *hostkey = NULL;  // hostkey
....
5808.       memset(&hostkey, 0, sizeof(hostkey));
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=795
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	5910	5917
Object	hostkey	sizeof

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL handle_SSH2_dh_gex_reply_after_known_hosts(PTInstVar pvar)

```
....
5910.       Key *hostkey = NULL;  // hostkey
....
5917.       memset(&hostkey, 0, sizeof(hostkey));
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=796
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-	TeraTermProject@@teraterm-teraterm-

	4_106-CVE-2023-48795-TP.c	4_106-CVE-2023-48795-TP.c
Line	6075	6081
Object	hostkey	sizeof

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method static BOOL handle_SSH2_ecdh_kex_reply(PTInstVar pvar)

```
....
6075.        Key *hostkey = NULL;  // hostkey
....
6081.        memset(&hostkey, 0, sizeof(hostkey));
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=797
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	6184	6189
Object	hostkey	sizeof

Code Snippet
File Name TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method BOOL handle_SSH2_ecdh_kex_reply_after_known_hosts(PTInstVar pvar)

```
....
6184.        Key *hostkey = NULL;  // hostkey
....
6189.        memset(&hostkey, 0, sizeof(hostkey));
```

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=1030073&projectid=30062&pathid=798
Status	New

The buffer allocated by <= in tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c at line 34 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Line	48	48
Object	<=	<=

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.2.0-CVE-2024-29040-TP.c
Method	ifapi_parse_json(const char *jstring) {

```
....
48.          for (char_pos = 0; char_pos <= tok->char_offset;
char_pos++) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=799
Status	New

The buffer allocated by <= in tpm2-software@@tpm2-tss-3.2.1-CVE-2024-29040-TP.c at line 34 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	tpm2-software@@tpm2-tss-3.2.1-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-3.2.1-CVE-2024-29040-TP.c
Line	48	48
Object	<=	<=

Code Snippet

File Name	tpm2-software@@tpm2-tss-3.2.1-CVE-2024-29040-TP.c
Method	ifapi_parse_json(const char *jstring) {

```
....
48.          for (char_pos = 0; char_pos <= tok->char_offset;
char_pos++) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=800
Status	New

The buffer allocated by <= in tpm2-software@@tpm2-tss-4.1.0-rc0-CVE-2024-29040-TP.c at line 34 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	tpm2-software@@tpm2-tss-4.1.0-rc0-CVE-2024-29040-TP.c	tpm2-software@@tpm2-tss-4.1.0-rc0-CVE-2024-29040-TP.c
Line	51	51
Object	<=	<=

Code Snippet

File Name	tpm2-software@@tpm2-tss-4.1.0-rc0-CVE-2024-29040-TP.c
Method	ifapi_parse_json(const char *jstring) {

```
....
51.          for (char_pos = 0; char_pos <= tok->char_offset;
char_pos++) {
```

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=1030073&projectid=30062&pathid=894
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4464	4464
Object	listed	sizeof

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void normalize_generic_order(char *buf, char default_strings[], int default_strings_len)

```
....
4464.       memset(listed, 0, sizeof(listed));
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=895
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	4465	4465
Object	allowed	sizeof

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	void normalize_generic_order(char *buf, char default_strings[], int default_strings_len)

```
....
4465.        memset(allowed, 0, sizeof(allowed));
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=896
Status	New

	Source	Destination
File	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Line	8774	8774
Object	msg	sizeof

Code Snippet

File Name	TeraTermProject@@teraterm-teraterm-4_106-CVE-2023-48795-TP.c
Method	static BOOL SSH2_scp_fromremote(PTInstVar pvar, Channel_t *c, unsigned char *data, unsigned int buflen)

```
....
8774.                   copylen = min(buflen, sizeof(msg));
```

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=1030073&projectid=30062&pathid=624
Status	New

Method place at line 281 of TheAlgorithms@@C-newest-CVE-2021-3520-FP.c uses a weak method rand 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	TheAlgorithms@@C-newest-CVE-2021-3520-FP.c	TheAlgorithms@@C-newest-CVE-2021-3520-FP.c
Line	284	284
Object	rand	rand

Code Snippet
File Name TheAlgorithms@@C-newest-CVE-2021-3520-FP.c
Method void place()

```
....
284.        int e = rand() % 9;
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1030073&projectid=30062&pathid=625
Status	New

Method main at line 37 of TheAlgorithms@@C-newest-CVE-2021-3520-FP.c uses a weak method srand 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	TheAlgorithms@@C-newest-CVE-2021-3520-FP.c	TheAlgorithms@@C-newest-CVE-2021-3520-FP.c
Line	39	39
Object	srand	srand

Code Snippet
File Name TheAlgorithms@@C-newest-CVE-2021-3520-FP.c
Method int main()

```
....
        srand( (unsigned int)time(NULL));
```

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

CPP

Overflowing Buffers

```cpp
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));
    }
}
```

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;
}
```

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);
```

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

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;
}
```

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

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 a One Way Hash without a Salt

Risk

What might happen

If an attacker gains access to the hashed passwords, she would likely be able to reverse the hash due to this weakness, and retrieve the original password. Once the passwords are discovered, the attacker can impersonate the users, and take full advantage of their privileges and access their personal data. Furthermore, this would likely not be discovered, as the attacker is being identified solely by the victims' credentials.

Cause

How does it happen

Typical cryptographic hashes, such as SHA-1 and MD5, are incredibly fast. Combined with attack techniques such as precomputed Rainbow Tables, it is relatively easy for attackers to reverse the hashes, and discover the original passwords. Lack of a unique, random salt added to the password makes brute force attacks even simpler.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.

- Do not use weak, outdated, or obsolete algorithms.

- Ensure you select the correct cryptographic mechanism according to the specific requirements.

Specific Recommendations:

- Passwords should be protected using a password hashing algorithm, instead of a general cryptographic hash. This includes adaptive hashes such as bcrypt, scrypt, PBKDF2 and Argon2.

- Tune the work factor, or cost, of the adaptive hash function according to the designated environment and risk profile.

- Do not use a regular cryptographic hash, such as SHA-1 or MD5, to protect passwords, as these are too fast.

- If it is necessary to use a common hash to protect passwords, add several bytes of unique, random data ("salt") to the password before hashing it. Store the salt with the hashed password, and do not reuse the same salt for multiple passwords.

Source Code Examples

Java

Unsalted Hashed Password

```
private String protectPassword(String password) {
      byte[] data = password.getBytes();
      byte[] hash = null;

      MessageDigest md = MessageDigest.getInstance("MD5");
      hash = md.digest(data);

      return Base64.getEncoder().encodeToString(hash);
}
```

Fast Hash with Salt

```
private String protectPassword(String password) {
      byte[] data = password.getBytes("UTF-8");
      byte[] hash = null;

      try {
             MessageDigest md = MessageDigest.getInstance("SHA-1");

             SecureRandom rand = new SecureRandom();
             byte[] salt = new byte[32];
             rand.nextBytes(salt);

             md.update(salt);
             md.update(data);

             hash = md.digest();
    }
      catch (GeneralSecurityException gse) {
             handleCryptoErrors(gse);
    }
      finally {
             Arrays.fill(data, 0);
    }

      return Base64.getEncoder().encodeToString(hash);
}
```

Slow, Adaptive Password Hash

```
private String protectPassword(String password) {
      byte[] data = password.getBytes("UTF-8");
      byte[] hash = null;

      try {
             SecureRandom rand = new SecureRandom();
             byte[] salt = new byte[32];
             rand.nextBytes(salt);

             SecretKeyFactory skf = SecretKeyFactory.getInstance("PBKDF2WithHmacSHA512");
             PBEKeySpec spec = new PBEKeySpec(data, salt, ITERATION_COUNT, KEY_LENGTH);
             // ITERATION_COUNT should be configured by environment, KEY_LENGTH should be 256
             SecretKey key = skf.generateSecret(spec);

             hash = key.getEncoded();
    }
      catch (GeneralSecurityException gse) {
             handleCryptoErrors(gse);
    }
      finally {
             Arrays.fill(data, 0);
    }

      return Base64.getEncoder().encodeToString(hash);
}
```

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());
```

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

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

Potential Precision Problem

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

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--;
                }
            }
        }
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025