vul_files_13 Scan Report

Project Name	vul_files_13
Scan Start	Monday, January 6, 2025 7:59:07 PM
Preset	Checkmarx Default
Scan Time	02h:05m:08s
Lines Of Code Scanned	299122
Files Scanned	143
Report Creation Time	Monday, January 6, 2025 10:50:19 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	1/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

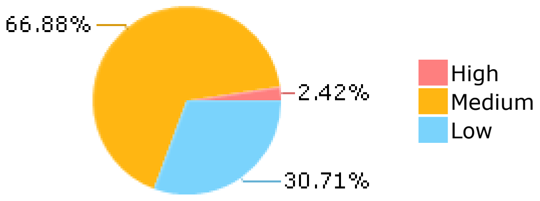
Results Limit

Results limit per query was set to 50

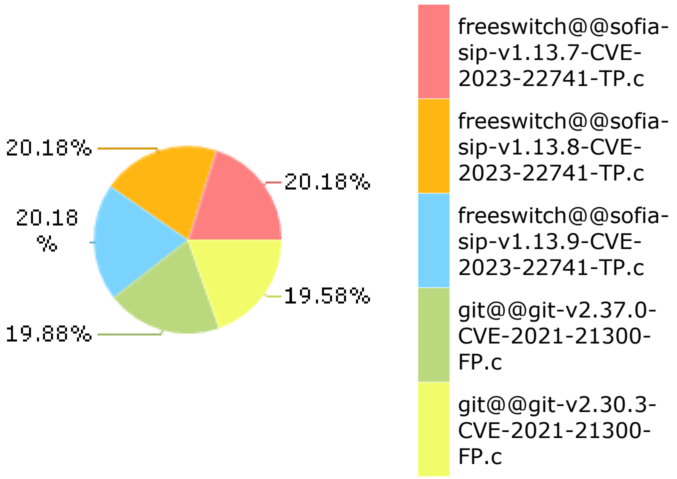
Selected Queries

Selected queries are listed in Result Summary

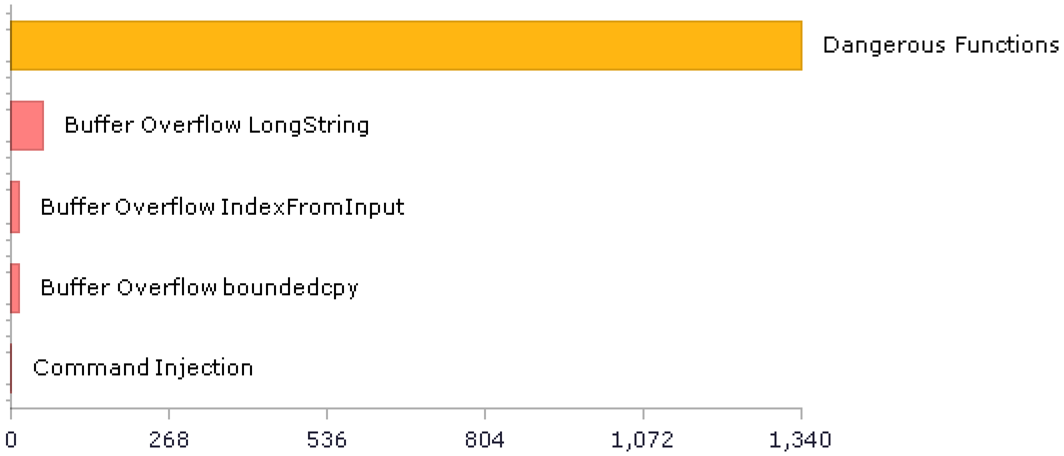
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	846	547
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	336	336
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	64	52
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	1356	1356
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	46	31
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	24	24
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	1356	1356
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	28	28
PCI DSS (3.2) - 6.5.2 - Buffer overflows	374	374
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.	84	84
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.	2	2
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.	20	6
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.	259	259
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.	46	43
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.	56	41

* 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)	340	338
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)	4	4
SC-13 Cryptographic Protection (P1)	28	13
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)	13	13
SC-4 Information in Shared Resources (P1)	34	34
SC-5 Denial of Service Protection (P1)*	731	347
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	199	160
SI-11 Error Handling (P2)*	228	228
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	28	28

***** 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

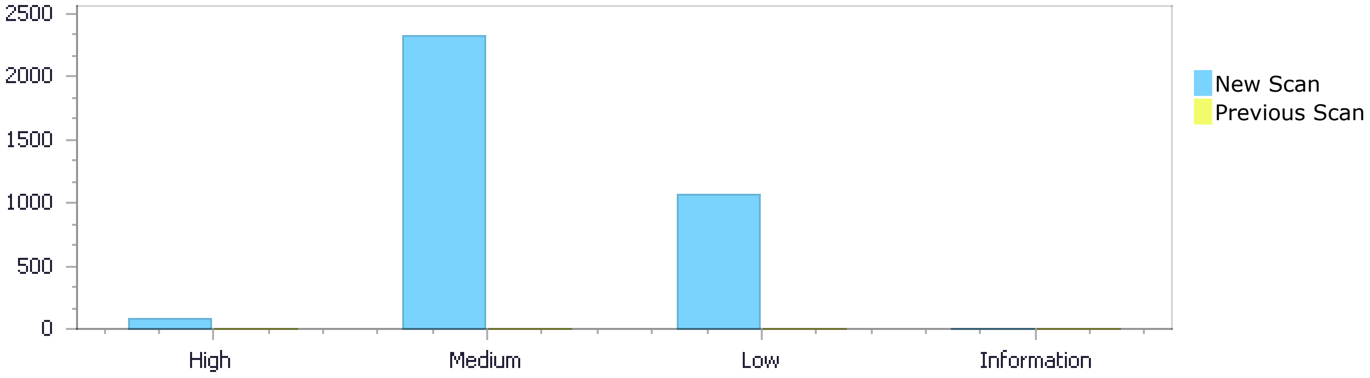
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	84	2,324	1,067	0	3,475
Recurrent Issues	0	0	0	0	0
Total	84	2,324	1,067	0	3,475

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	84	2,324	1,067	0	3,475
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	84	2,324	1,067	0	3,475

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow LongString	56	High
Buffer Overflow IndexFromInput	15	High
Buffer Overflow boundedcpy	12	High
Command Injection	1	High
Dangerous Functions	1341	Medium

Buffer Overflow boundcpy WrongSizeParam	295	Medium
Use of Zero Initialized Pointer	253	Medium
MemoryFree on StackVariable	129	Medium
Memory Leak	119	Medium
Environment Injection	45	Medium
Stored Buffer Overflow boundcpy	36	Medium
Wrong Size t Allocation	34	Medium
Heap Inspection	24	Medium
Inadequate Encryption Strength	16	Medium
Use of a One Way Hash without a Salt	12	Medium
Integer Overflow	10	Medium
Use of Uninitialized Variable	5	Medium
Use of Hard coded Cryptographic Key	4	Medium
Off by One Error in Methods	1	Medium
NULL Pointer Dereference	352	Low
Improper Resource Access Authorization	252	Low
Unchecked Return Value	228	Low
Incorrect Permission Assignment For Critical Resources	84	Low
Unchecked Array Index	33	Low
TOCTOU	30	Low
Potential Off by One Error in Loops	27	Low
Use of Obsolete Functions	15	Low
Insecure Temporary File	10	Low
Use of Insufficiently Random Values	10	Low
Inconsistent Implementations	8	Low
Potential Precision Problem	6	Low
Exposure of System Data to Unauthorized Control Sphere	4	Low
Information Exposure Through Comments	3	Low
Use of Sizeof On a Pointer Type	3	Low
Arithmenic Operation On Boolean	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	56
FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	56
freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	53
freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	53
freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	53
git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	46
git@@git-v2.39.5-CVE-2021-21300-FP.c	46
git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	46
git@@git-v2.42.0-CVE-2021-21300-FP.c	46
git@@git-v2.43.1-CVE-2021-21300-FP.c	46

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=1000020&projectid=15&pathid=28
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	730	731
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                snprintf(c, sizeof(c), "%02x",
data[i]);
731.                                strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=29
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	724	726
Object	" %02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                                   snprintf(c, sizeof(c), " %02x",
....
726.                                   strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=30
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	1728	1730
Object	"%02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1728.                                  snprintf(c, sizeof(c), "%02x",
....
1730.                                  strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=31
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	1722	1724
Object	" %02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1722.                                snprintf(c, sizeof(c), " %02x",
....
1724.                                strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=32
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	730	731
Object	"%02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                 snprintf(c, sizeof(c), "%02x",
data[i]);
731.                                 strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=33
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	724	726
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                                    snprintf(c, sizeof(c), " %02x",
....
726.                                    strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=34
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	1728	1730
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1728.                                   snprintf(c, sizeof(c), "%02x",
....
1730.                                   strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=35
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	1722	1724
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1722.                                   snprintf(c, sizeof(c), " %02x",
....
1724.                                   strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=36
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	730	731
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                    snprintf(c, sizeof(c), "%02x",
data[i]);
731.                                    strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=37
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	724	726
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                                    snprintf(c, sizeof(c), " %02x",
....
726.                                    strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=38
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2024-	FRRouting@@frr-frr-7.2.1-CVE-2024-

	31949-TP.c	31949-TP.c
Line	1728	1730
Object	"%02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1728.                                   snprintf(c, sizeof(c), "%02x",
....
1730.                                   strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=39
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	1722	1724
Object	" %02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1722.                                   snprintf(c, sizeof(c), " %02x",
....
1724.                                   strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=40
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	730	731
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                    snprintf(c, sizeof(c), "%02x",
data[i]);
731.                                    strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=41
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	724	726
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                                    snprintf(c, sizeof(c), " %02x",
....
726.                                    strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=42
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	1730	1732
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1730.                                  snprintf(c, sizeof(c), "%02x",
....
1732.                                  strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=43
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	1724	1726
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1724.                                  snprintf(c, sizeof(c), " %02x",
....
1726.                                  strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=44
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	730	731
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                    snprintf(c, sizeof(c), "%02x",
data[i]);
731.                                    strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=45
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	724	726
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                                    snprintf(c, sizeof(c), " %02x",
....
726.                                    strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=46
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	1730	1732
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1730.                                   snprintf(c, sizeof(c), "%02x",
....
1732.                                   strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=47
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	1724	1726
Object	" %02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1724.                                  snprintf(c, sizeof(c), " %02x",
....
1726.                                  strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=48
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	730	731
Object	"%02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                   snprintf(c, sizeof(c), "%02x",
data[i]);
731.                                   strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=49
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2024-	FRRouting@@frr-frr-7.3.1-CVE-2024-

	31949-TP.c	31949-TP.c
Line	724	726
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                                            snprintf(c, sizeof(c), " %02x",
....
726.                                            strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=50
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	1730	1732
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1730.                                           snprintf(c, sizeof(c), "%02x",
....
1732.                                           strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=51
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	1724	1726
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1724.                              snprintf(c, sizeof(c), " %02x",
....
1726.                              strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=52
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	750	752
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
750.                               snprintf(c, sizeof(c), "%02x",
data[i]);
....
752.                               strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=53
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	742	745
Object	" %02x"	c

Code Snippet

File Name FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c

Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
742.                                    snprintf(c, sizeof(c), " %02x",
....
745.                                    strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=54
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	1840	1843
Object	"%02x"	c

Code Snippet

File Name FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c

Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1840.                                   snprintf(c, sizeof(c), "%02x",
....
1843.                                   strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=55
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	1832	1835
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1832.                                   snprintf(c, sizeof(c), " %02x",
....
1835.                                   strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=56
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Line	750	752
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
750.                                    snprintf(c, sizeof(c), "%02x",
data[i]);
....
752.                                    strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=57
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Line	742	745
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
742.                                    snprintf(c, sizeof(c), " %02x",
....
745.                                    strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=58
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Line	1840	1843

Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1840.                                   snprintf(c, sizeof(c), "%02x",
....
1843.                                   strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=59
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Line	1832	1835
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1832.                                   snprintf(c, sizeof(c), " %02x",
....
1835.                                   strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=60
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Line	750	752
Object	"%02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
750.                                    snprintf(c, sizeof(c), "%02x",
data[i]);
....
752.                                    strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=61
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Line	742	745
Object	" %02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
742.                                    snprintf(c, sizeof(c), " %02x",
....
745.                                    strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=62
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Line	1840	1843
Object	"%02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1840.                                   snprintf(c, sizeof(c), "%02x",
....
1843.                                   strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=63
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Line	1832	1835
Object	" %02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1832.                                   snprintf(c, sizeof(c), " %02x",
....
1835.                                   strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 37:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=64
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Line	789	791
Object	"%02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
789.                                snprintf(c, sizeof(c), "%02x",
data[i]);
....
791.                                strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=65
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Line	781	784
Object	" %02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
781.                                snprintf(c, sizeof(c), " %02x",
....
784.                                strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=66
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Line	1890	1893
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1890.                               snprintf(c, sizeof(c), "%02x",
....
1893.                               strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=67
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Line	1882	1885
Object	" %02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1882.                                  snprintf(c, sizeof(c), " %02x",
....
1885.                                  strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=68
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c
Line	789	791
Object	"%02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
789.                                   snprintf(c, sizeof(c), "%02x",
data[i]);
....
791.                                   strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=69
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination

File	FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c
Line	781	784
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
781.                                          snprintf(c, sizeof(c), " %02x",
....
784.                                          strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 43:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=70
Status New

The size of the buffer used by bgp_notify_receive in c, at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c
Line	1890	1893
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1890.                                         snprintf(c, sizeof(c), "%02x",
....
1893.                                         strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 44:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=71
Status New

The size of the buffer used by bgp_notify_receive in c, at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c
Line	1882	1885
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-47234-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1882.                                    snprintf(c, sizeof(c), " %02x",
....
1885.                                    strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=72
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to "%02x", at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c
Line	789	791
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
789.                                     snprintf(c, sizeof(c), "%02x",
data[i]);
....
791.                                     strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 46:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=73
Status	New

The size of the buffer used by bgp_notify_send_with_data in c, at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_with_data passes to " %02x", at line 719 of FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c
Line	781	784
Object	" %02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
781.                                    snprintf(c, sizeof(c), " %02x",
....
784.                                    strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=74
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to "%02x", at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c
Line	1890	1893
Object	"%02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1890.                                    snprintf(c, sizeof(c), "%02x",
....
1893.                                    strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=75
Status	New

The size of the buffer used by bgp_notify_receive in c, at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_receive passes to " %02x", at line 1846 of FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c
Line	1882	1885
Object	" %02x"	c

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2024-31949-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1882.                                    snprintf(c, sizeof(c), " %02x",
....
1885.                                    strlcat(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=76
Status	New

The size of the buffer used by bgp_notify_send_internal in c, at line 909 of FRRouting@@frr-frr-8.4.4-CVE-2023-47234-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_internal passes to "%02x", at line 909 of FRRouting@@frr-frr-8.4.4-CVE-2023-47234-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-47234-FP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-47234-FP.c
Line	996	998
Object	"%02x"	c

Code Snippet
File Name FRRouting@@frr-frr-8.4.4-CVE-2023-47234-FP.c
Method static void bgp_notify_send_internal(struct peer *peer, uint8_t code,

```
....
996.                            snprintf(c, sizeof(c), "%02x",
data[i]);
....
998.                            strlcpy(bgp_notify.data, c,
```

Buffer Overflow LongString\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=77
Status	New

The size of the buffer used by bgp_notify_send_internal in c, at line 909 of FRRouting@@frr-frr-8.4.4-CVE-2023-47234-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_notify_send_internal passes to " %02x", at line 909 of FRRouting@@frr-frr-8.4.4-CVE-2023-47234-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-47234-FP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-47234-FP.c
Line	988	991
Object	" %02x"	c

Code Snippet
File Name FRRouting@@frr-frr-8.4.4-CVE-2023-47234-FP.c
Method static void bgp_notify_send_internal(struct peer *peer, uint8_t code,

```
....
988.                            snprintf(c, sizeof(c), " %02x",
....
991.                            strlcat(bgp_notify.data, c,
```

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=1000020&projectid=15&pathid=13

Status	New

The size of the buffer used by *parse_interpreter in n, at line 1176 of git@@git-v2.26.0-rc1-CVE-2021-21300-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_interpreter passes to buf, at line 1176 of git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	1190	1197
Object	buf	n

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1190.        n = read(fd, buf, sizeof(buf)-1);
....
1197.        buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=14
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1198 of git@@git-v2.28.0-rc0-CVE-2021-21300-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_interpreter passes to buf, at line 1198 of git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	1212	1219
Object	buf	n

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1212.        n = read(fd, buf, sizeof(buf)-1);
....
1219.        buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=15
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1201 of git@@git-v2.29.0-rc2-CVE-2021-21300-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_interpreter passes to buf, at line 1201 of git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	1215	1222
Object	buf	n

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1215.         n = read(fd, buf, sizeof(buf)-1);
....
1222.         buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=16
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1201 of git@@git-v2.30.1-CVE-2021-21300-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_interpreter passes to buf, at line 1201 of git@@git-v2.30.1-CVE-2021-21300-TP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	1215	1222
Object	buf	n

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1215.        n = read(fd, buf, sizeof(buf)-1);
....
1222.        buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=17
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1206 of git@@git-v2.30.3-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1206 of git@@git-v2.30.3-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	1220	1227
Object	buf	n

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1220.        n = read(fd, buf, sizeof(buf)-1);
....
1227.        buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=18
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1206 of git@@git-v2.30.8-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1206 of git@@git-v2.30.8-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	1220	1227
Object	buf	n

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1220.         n = read(fd, buf, sizeof(buf)-1);
....
1227.         buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=19
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1205 of git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1205 of git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	1219	1226
Object	buf	n

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1219.         n = read(fd, buf, sizeof(buf)-1);
....
1226.         buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=20
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1226 of git@@git-v2.33.0-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1226 of git@@git-v2.33.0-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c

Line	1240	1247
Object	buf	n

Code Snippet

File Name	git@@git-v2.33.0-CVE-2021-21300-FP.c
Method	static const char *parse_interpreter(const char *cmd)

```
....
1240.        n = read(fd, buf, sizeof(buf)-1);
....
1247.        buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=21
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1226 of git@@git-v2.34.1-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1226 of git@@git-v2.34.1-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	1240	1247
Object	buf	n

Code Snippet

File Name	git@@git-v2.34.1-CVE-2021-21300-FP.c
Method	static const char *parse_interpreter(const char *cmd)

```
....
1240.        n = read(fd, buf, sizeof(buf)-1);
....
1247.        buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=22
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1250 of git@@git-v2.37.0-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1250 of git@@git-v2.37.0-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	1264	1271
Object	buf	n

Code Snippet
File Name git@@git-v2.37.0-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1264.         n = read(fd, buf, sizeof(buf)-1);
....
1271.         buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=23
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1248 of git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1248 of git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	1262	1269
Object	buf	n

Code Snippet
File Name git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1262.         n = read(fd, buf, sizeof(buf)-1);
....
1269.         buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=24
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1251 of git@@git-v2.39.5-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1251 of git@@git-v2.39.5-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	1265	1272
Object	buf	n

Code Snippet
File Name	git@@git-v2.39.5-CVE-2021-21300-FP.c
Method	static const char *parse_interpreter(const char *cmd)

```
....
1265.         n = read(fd, buf, sizeof(buf)-1);
....
1272.         buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=25
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1258 of git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1258 of git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	1272	1279
Object	buf	n

Code Snippet
File Name	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method	static const char *parse_interpreter(const char *cmd)

```
....
1272.         n = read(fd, buf, sizeof(buf)-1);
....
1279.         buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 14:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=26
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1258 of git@@git-v2.42.0-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1258 of git@@git-v2.42.0-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	1272	1279
Object	buf	n

Code Snippet

File Name	git@@git-v2.42.0-CVE-2021-21300-FP.c
Method	static const char *parse_interpreter(const char *cmd)

```
....
1272.        n = read(fd, buf, sizeof(buf)-1);
....
1279.        buf[n] = '\0';
```

Buffer Overflow IndexFromInput\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=27
Status	New

The size of the buffer used by *parse_interpreter in n, at line 1260 of git@@git-v2.43.1-CVE-2021-21300-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *parse_interpreter passes to buf, at line 1260 of git@@git-v2.43.1-CVE-2021-21300-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	1274	1281
Object	buf	n

Code Snippet

File Name	git@@git-v2.43.1-CVE-2021-21300-FP.c
Method	static const char *parse_interpreter(const char *cmd)

```
....
1274.        n = read(fd, buf, sizeof(buf)-1);
....
1281.        buf[n] = '\0';
```

Buffer Overflow boundedcpy

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundedcpy 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 boundedcpy\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=4
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.30.1-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.30.1-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.30.1-CVE-2020-5260-FP.c	git@@git-v2.30.1-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet

File Name	git@@git-v2.30.1-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.30.1-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=5
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.30.3-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.30.3-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.30.3-CVE-2020-5260-FP.c	git@@git-v2.30.3-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet
File Name git@@git-v2.30.3-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.30.3-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=6
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.30.8-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.30.8-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.30.8-CVE-2020-5260-FP.c	git@@git-v2.30.8-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet
File Name git@@git-v2.30.8-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.30.8-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.          memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=7
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet

File Name git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.          while (fgets(buf, 1024, stdin)) {
```

▼

File Name git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.          memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=8
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.33.0-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.33.0-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination

File	git@@git-v2.33.0-CVE-2020-5260-FP.c	git@@git-v2.33.0-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet
File Name git@@git-v2.33.0-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.33.0-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.         memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=9
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.34.1-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.34.1-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.34.1-CVE-2020-5260-FP.c	git@@git-v2.34.1-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet
File Name git@@git-v2.34.1-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.34.1-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=10
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.37.0-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.37.0-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.37.0-CVE-2020-5260-FP.c	git@@git-v2.37.0-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet

File Name git@@git-v2.37.0-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

▼

File Name git@@git-v2.37.0-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=11
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2020-5260-	git@@git-v2.38.0-rc2-CVE-2020-5260-

	FP.c	FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet
File Name git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Buffer Overflow boundedcpy\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=12
Status	New

The size parameter sizeof in line 330 in file git@@git-v2.39.5-CVE-2020-5260-FP.c is influenced by the user input stdin in line 346 in file git@@git-v2.39.5-CVE-2020-5260-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	git@@git-v2.39.5-CVE-2020-5260-FP.c	git@@git-v2.39.5-CVE-2020-5260-FP.c
Line	355	332
Object	stdin	sizeof

Code Snippet
File Name git@@git-v2.39.5-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.39.5-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Command Injection

Query Path:
CPP\Cx\CPP High Risk\Command Injection Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Command Injection\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=379
Status	New

The application's main method calls an OS (shell) command with execv, at line 917 of FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, argv, which is retrieved by the application in the main method, at line 917 of FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	917	1059
Object	argv	execv

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method int main(int argc, char **argv)

```
....
917.  int main(int argc, char **argv)
....
1059.       execv(startas, argv);
```

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=1000020&projectid=15&pathid=425
Status	New

The dangerous function, memcpy, was found in use at line 82 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	92	92
Object	memcpy	memcpy

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_parse_message(stun_msg_t *msg)

```
....
92.     memcpy(msg->stun_hdr.tran_id, p + 4, STUN_TID_BYTES);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=426
Status	New

The dangerous function, memcpy, was found in use at line 114 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	182	182
Object	memcpy	memcpy

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_parse_attribute(stun_msg_t *msg, unsigned char *p)

```
....
182.        memcpy(attr->enc_buf.data, p, len);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=427
Status	New

The dangerous function, memcpy, was found in use at line 200 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	222	222
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_parse_attr_address(stun_attr_t *attr,

```
....
222.      memcpy(&addr->su_sin.sin_port, p + 2, 2);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=428
Status	New

The dangerous function, memcpy, was found in use at line 200 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	223	223
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c

Method int stun_parse_attr_address(stun_attr_t *attr,

```
....
223.    memcpy(&addr->su_sin.sin_addr.s_addr, p + 4, 4);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=429
Status	New

The dangerous function, memcpy, was found in use at line 235 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	240	240
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_parse_attr_error_code(stun_attr_t *attr, const unsigned char *p, unsigned len) {

```
....
240.    memcpy(&tmp, p, sizeof(uint32_t));
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=430
Status	New

The dangerous function, memcpy, was found in use at line 257 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	262	262
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_parse_attr_uint32(stun_attr_t *attr, const unsigned char *p, unsigned len)

```
....
262.    memcpy(&tmp, p, sizeof(uint32_t));
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=431
Status	New

The dangerous function, memcpy, was found in use at line 270 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	276	276
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_parse_attr_buffer(stun_attr_t *attr, const unsigned char *p, unsigned len)

```
....
276.    memcpy(buf->data, p, len);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=432
Status	New

The dangerous function, memcpy, was found in use at line 314 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	318	318

Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_copy_buffer(stun_buffer_t *p, stun_buffer_t *p2) {

```
....
318.     memcpy(p->data, p2->data, p->size);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=433
Status	New

The dangerous function, memcpy, was found in use at line 355 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	366	366
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_address(stun_attr_t *attr) {

```
....
366.     memcpy(attr->enc_buf.data+4, &tmp, sizeof(tmp));
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=434
Status	New

The dangerous function, memcpy, was found in use at line 355 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c

Line	367	367
Object	memcpy	memcpy

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_encode_address(stun_attr_t *attr) {

```
....
367.     memcpy(attr->enc_buf.data+6, &a->sin_port, 2);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=435
Status	New

The dangerous function, memcpy, was found in use at line 355 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	368	368
Object	memcpy	memcpy

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_encode_address(stun_attr_t *attr) {

```
....
368.     memcpy(attr->enc_buf.data+8, &a->sin_addr.s_addr, 4);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=436
Status	New

The dangerous function, memcpy, was found in use at line 373 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-	freeswitch@@sofia-sip-v1.13.7-CVE-

	2023-22741-TP.c	2023-22741-TP.c
Line	381	381
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_uint32(stun_attr_t *attr) {

```
....
381.    memcpy(attr->enc_buf.data+4, &tmp, 4);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=437
Status	New

The dangerous function, memcpy, was found in use at line 385 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	412	412
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_error_code(stun_attr_t *attr) {

```
....
412.      memcpy(attr->enc_buf.data+8, error->phrase,
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=438
Status	New

The dangerous function, memcpy, was found in use at line 420 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	429	429
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_buffer(stun_attr_t *attr) {

```
....
429.     memcpy(attr->enc_buf.data+4, a->data, a->size);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=439
Status	New

The dangerous function, memcpy, was found in use at line 434 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	452	452
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
452.       memcpy(padded_text, buf, len);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=440
Status	New

The dangerous function, memcpy, was found in use at line 434 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	463	463
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
463.    memcpy(attr->enc_buf.data + 4, sha1_hmac, 20);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=441
Status	New

The dangerous function, memcpy, was found in use at line 478 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	485	485
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_type_len(stun_attr_t *attr, uint16_t len) {

```
....
485.    memcpy(attr->enc_buf.data, &tmp, 2);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=442
Status	New

The dangerous function, memcpy, was found in use at line 478 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	488	488
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_type_len(stun_attr_t *attr, uint16_t len) {

```
....
488.     memcpy(attr->enc_buf.data + 2, &tmp, 2);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=443
Status	New

The dangerous function, memcpy, was found in use at line 499 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	529	529
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_validate_message_integrity(stun_msg_t *msg, stun_buffer_t *pwd)

```
....
529.     memcpy(padded_text, msg->enc_buf.data, len);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=444
Status	New

The dangerous function, memcpy, was found in use at line 499 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	531	531
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_validate_message_integrity(stun_msg_t *msg, stun_buffer_t *pwd)

```
....
531.    memcpy(dig, HMAC(EVP_sha1(), pwd->data, pwd->size, padded_text, 
padded_len, NULL, &dig_len), 20);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=445
Status	New

The dangerous function, memcpy, was found in use at line 660 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	724	724
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_message(stun_msg_t *msg, stun_buffer_t *pwd) {

```
....
724.      memcpy(buf + 4, msg->stun_hdr.tran_id, STUN_TID_BYTES);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=446
Status	New

The dangerous function, memcpy, was found in use at line 660 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	733	733
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_message(stun_msg_t *msg, stun_buffer_t *pwd) {

```
....
733.        memcpy(buf+len, (void *)attr->enc_buf.data, attr->enc_buf.size);
```

Dangerous Functions\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=447
Status New

The dangerous function, memcpy, was found in use at line 660 in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	745	745
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_message(stun_msg_t *msg, stun_buffer_t *pwd) {

```
....
745.        memcpy(buf+len, (void *)msg_int->enc_buf.data,
```

Dangerous Functions\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=448

Status	New

The dangerous function, memcpy, was found in use at line 82 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	92	92
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_parse_message(stun_msg_t *msg)

```
....
92.     memcpy(msg->stun_hdr.tran_id, p + 4, STUN_TID_BYTES);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=449
Status	New

The dangerous function, memcpy, was found in use at line 114 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	182	182
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_parse_attribute(stun_msg_t *msg, unsigned char *p)

```
....
182.       memcpy(attr->enc_buf.data, p, len);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=450
Status	New

The dangerous function, memcpy, was found in use at line 200 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	222	222
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_parse_attr_address(stun_attr_t *attr,

```
....
222.    memcpy(&addr->su_sin.sin_port, p + 2, 2);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=451
Status	New

The dangerous function, memcpy, was found in use at line 200 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	223	223
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_parse_attr_address(stun_attr_t *attr,

```
....
223.    memcpy(&addr->su_sin.sin_addr.s_addr, p + 4, 4);
```

Dangerous Functions\Path 28:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=452
Status	New

The dangerous function, memcpy, was found in use at line 235 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	240	240
Object	memcpy	memcpy

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	int stun_parse_attr_error_code(stun_attr_t *attr, const unsigned char *p, unsigned len) {

```
....
240.     memcpy(&tmp, p, sizeof(uint32_t));
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=453
Status	New

The dangerous function, memcpy, was found in use at line 257 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	262	262
Object	memcpy	memcpy

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	int stun_parse_attr_uint32(stun_attr_t *attr, const unsigned char *p, unsigned len)

```
....
262.     memcpy(&tmp, p, sizeof(uint32_t));
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=454
Status	New

The dangerous function, memcpy, was found in use at line 270 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	276	276
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_parse_attr_buffer(stun_attr_t *attr, const unsigned char *p, unsigned len)

```
....
276.    memcpy(buf->data, p, len);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=455
Status	New

The dangerous function, memcpy, was found in use at line 314 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	318	318
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_copy_buffer(stun_buffer_t *p, stun_buffer_t *p2) {

```
....
318.    memcpy(p->data, p2->data, p->size);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=456
Status	New

The dangerous function, memcpy, was found in use at line 355 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	366	366
Object	memcpy	memcpy

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	int stun_encode_address(stun_attr_t *attr) {

```
....
366.     memcpy(attr->enc_buf.data+4, &tmp, sizeof(tmp));
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=457
Status	New

The dangerous function, memcpy, was found in use at line 355 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	367	367
Object	memcpy	memcpy

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	int stun_encode_address(stun_attr_t *attr) {

```
....
367.    memcpy(attr->enc_buf.data+6, &a->sin_port, 2);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=458
Status	New

The dangerous function, memcpy, was found in use at line 355 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	368	368
Object	memcpy	memcpy

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	int stun_encode_address(stun_attr_t *attr) {

```
....
368.    memcpy(attr->enc_buf.data+8, &a->sin_addr.s_addr, 4);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=459
Status	New

The dangerous function, memcpy, was found in use at line 373 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	381	381
Object	memcpy	memcpy

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c

Method int stun_encode_uint32(stun_attr_t *attr) {

```
....
381.     memcpy(attr->enc_buf.data+4, &tmp, 4);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=460
Status	New

The dangerous function, memcpy, was found in use at line 385 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	412	412
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_error_code(stun_attr_t *attr) {

```
....
412.       memcpy(attr->enc_buf.data+8, error->phrase,
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=461
Status	New

The dangerous function, memcpy, was found in use at line 420 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	429	429
Object	memcpy	memcpy

Code Snippet

File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_buffer(stun_attr_t *attr) {

```
....
429.     memcpy(attr->enc_buf.data+4, a->data, a->size);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=462
Status	New

The dangerous function, memcpy, was found in use at line 434 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	452	452
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
452.       memcpy(padded_text, buf, len);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=463
Status	New

The dangerous function, memcpy, was found in use at line 434 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	463	463
Object	memcpy	memcpy

Code Snippet	
File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	int stun_encode_message_integrity(stun_attr_t *attr,

```
....
463.     memcpy(attr->enc_buf.data + 4, sha1_hmac, 20);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=464
Status	New

The dangerous function, memcpy, was found in use at line 478 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	485	485
Object	memcpy	memcpy

Code Snippet	
File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	int stun_encode_type_len(stun_attr_t *attr, uint16_t len) {

```
....
485.     memcpy(attr->enc_buf.data, &tmp, 2);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=465
Status	New

The dangerous function, memcpy, was found in use at line 478 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	488	488
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_type_len(stun_attr_t *attr, uint16_t len) {

```
....
488.    memcpy(attr->enc_buf.data + 2, &tmp, 2);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=466
Status	New

The dangerous function, memcpy, was found in use at line 499 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	529	529
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_validate_message_integrity(stun_msg_t *msg, stun_buffer_t *pwd)

```
....
529.    memcpy(padded_text, msg->enc_buf.data, len);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=467
Status	New

The dangerous function, memcpy, was found in use at line 499 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	531	531

Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_validate_message_integrity(stun_msg_t *msg, stun_buffer_t *pwd)

```
....
531.     memcpy(dig, HMAC(EVP_sha1(), pwd->data, pwd->size, padded_text, 
padded_len, NULL, &dig_len), 20);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=468
Status	New

The dangerous function, memcpy, was found in use at line 660 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	724	724
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_message(stun_msg_t *msg, stun_buffer_t *pwd) {

```
....
724.       memcpy(buf + 4, msg->stun_hdr.tran_id, STUN_TID_BYTES);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=469
Status	New

The dangerous function, memcpy, was found in use at line 660 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c

Line	733	733
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_message(stun_msg_t *msg, stun_buffer_t *pwd) {

```
....
733.         memcpy(buf+len, (void *)attr->enc_buf.data, attr-
>enc_buf.size);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=470
Status	New

The dangerous function, memcpy, was found in use at line 660 in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	745	745
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_message(stun_msg_t *msg, stun_buffer_t *pwd) {

```
....
745.         memcpy(buf+len, (void *)msg_int->enc_buf.data,
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=471
Status	New

The dangerous function, memcpy, was found in use at line 82 in freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	92	92
Object	memcpy	memcpy

Code Snippet

File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c

Method int stun_parse_message(stun_msg_t *msg)

```
....
92.     memcpy(msg->stun_hdr.tran_id, p + 4, STUN_TID_BYTES);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=472
Status	New

The dangerous function, memcpy, was found in use at line 114 in freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	182	182
Object	memcpy	memcpy

Code Snippet

File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c

Method int stun_parse_attribute(stun_msg_t *msg, unsigned char *p)

```
....
182.       memcpy(attr->enc_buf.data, p, len);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=473
Status	New

The dangerous function, memcpy, was found in use at line 200 in freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	222	222
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method int stun_parse_attr_address(stun_attr_t *attr,

```
....
222.     memcpy(&addr->su_sin.sin_port, p + 2, 2);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=474
Status	New

The dangerous function, memcpy, was found in use at line 200 in freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	223	223
Object	memcpy	memcpy

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method int stun_parse_attr_address(stun_attr_t *attr,

```
....
223.     memcpy(&addr->su_sin.sin_addr.s_addr, p + 4, 4);
```

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=1000020&projectid=15&pathid=84
Status	New

The size of the buffer used by stun_parse_attr_error_code in uint32_t, at line 235 of freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stun_parse_attr_error_code passes to uint32_t, at line 235 of freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c, to overwrite the target buffer.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	240	240
Object	uint32_t	uint32_t

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_parse_attr_error_code(stun_attr_t *attr, const unsigned char *p, unsigned len) {

```
....
240.     memcpy(&tmp, p, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=85
Status	New

The size of the buffer used by stun_parse_attr_uint32 in uint32_t, at line 257 of freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stun_parse_attr_uint32 passes to uint32_t, at line 257 of freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c, to overwrite the target buffer.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	262	262
Object	uint32_t	uint32_t

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_parse_attr_uint32(stun_attr_t *attr, const unsigned char *p, unsigned len)

```
....
262.     memcpy(&tmp, p, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=86
Status	New

The size of the buffer used by stun_encode_address in tmp, at line 355 of freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stun_encode_address passes to tmp, at line 355 of freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c, to overwrite the target buffer.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	366	366
Object	tmp	tmp

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_address(stun_attr_t *attr) {

```
....
366.    memcpy(attr->enc_buf.data+4, &tmp, sizeof(tmp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=87
Status	New

The size of the buffer used by stun_parse_attr_error_code in uint32_t, at line 235 of freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stun_parse_attr_error_code passes to uint32_t, at line 235 of freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c, to overwrite the target buffer.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	240	240
Object	uint32_t	uint32_t

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_parse_attr_error_code(stun_attr_t *attr, const unsigned char *p, unsigned len) {

```
....
240.    memcpy(&tmp, p, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=88
Status	New

The size of the buffer used by stun_parse_attr_uint32 in uint32_t, at line 257 of freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stun_parse_attr_uint32 passes to uint32_t, at line 257 of freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c, to overwrite the target buffer.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	262	262
Object	uint32_t	uint32_t

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	int stun_parse_attr_uint32(stun_attr_t *attr, const unsigned char *p, unsigned len)

```
....
262.    memcpy(&tmp, p, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=89
Status	New

The size of the buffer used by stun_encode_address in tmp, at line 355 of freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stun_encode_address passes to tmp, at line 355 of freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c, to overwrite the target buffer.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	366	366
Object	tmp	tmp

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	int stun_encode_address(stun_attr_t *attr) {

```
....
366.    memcpy(attr->enc_buf.data+4, &tmp, sizeof(tmp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=90
Status	New

The size of the buffer used by stun_parse_attr_error_code in uint32_t, at line 235 of freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stun_parse_attr_error_code passes to uint32_t, at line 235 of freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c, to overwrite the target buffer.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	240	240
Object	uint32_t	uint32_t

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method	int stun_parse_attr_error_code(stun_attr_t *attr, const unsigned char *p, unsigned len) {

```
....
240.    memcpy(&tmp, p, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=91
Status	New

The size of the buffer used by stun_parse_attr_uint32 in uint32_t, at line 257 of freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stun_parse_attr_uint32 passes to uint32_t, at line 257 of freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c, to overwrite the target buffer.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	262	262
Object	uint32_t	uint32_t

Code Snippet	
File Name	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method	int stun_parse_attr_uint32(stun_attr_t *attr, const unsigned char *p, unsigned len)

```
....
262.     memcpy(&tmp, p, sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=92
Status	New

The size of the buffer used by stun_encode_address in tmp, at line 355 of freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stun_encode_address passes to tmp, at line 355 of freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c, to overwrite the target buffer.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	366	366
Object	tmp	tmp

Code Snippet	
File Name	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method	int stun_encode_address(stun_attr_t *attr) {

```
....
366.     memcpy(attr->enc_buf.data+4, &tmp, sizeof(tmp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=93
Status	New

The size of the buffer used by really_send_update in ->, at line 1032 of FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1032 of FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c

Line	1100	1100
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c
Method really_send_update(struct interface *ifp,

```
....
1100.           memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=94
Status	New

The size of the buffer used by really_send_update in ->, at line 1032 of FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1032 of FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c
Line	1100	1100
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c
Method really_send_update(struct interface *ifp,

```
....
1100.           memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=95
Status	New

The size of the buffer used by really_send_update in ->, at line 1032 of FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1032 of FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c
Line	1100	1100
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c
Method really_send_update(struct interface *ifp,

```
....
1100.          memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=96
Status	New

The size of the buffer used by bgp_route_refresh_receive in uint32_t, at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to uint32_t, at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	1900	1900
Object	uint32_t	uint32_t

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1900.                                                  sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=97
Status	New

The size of the buffer used by bgp_capability_msg_parse in capability_mp_data, at line 2045 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer.

This can enable a buffer overflow attack, using the source buffer that bgp_capability_msg_parse passes to capability_mp_data, at line 2045 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	2092	2092
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,

```
....
2092.            memcpy(&mpc, pnt + 3, sizeof(struct 
capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=98
Status	New

The size of the buffer used by bgp_capability_vty_out in capability_mp_data, at line 55 of FRRouting@@frr-frr-7.2.1-CVE-2023-31489-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_vty_out passes to capability_mp_data, at line 55 of FRRouting@@frr-frr-7.2.1-CVE-2023-31489-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-31489-FP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-31489-FP.c
Line	78	78
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-31489-FP.c
Method void bgp_capability_vty_out(struct vty *vty, struct peer *peer, bool use_json,

```
....
78.        memcpy(&mpc, pnt + 2, sizeof(struct capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=99
Status	New

The size of the buffer used by really_send_update in ->, at line 1032 of FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1032 of FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c
Line	1100	1100
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c
Method really_send_update(struct interface *ifp,

```
....
1100.           memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp->buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=100
Status	New

The size of the buffer used by bgp_capability_vty_out in capability_mp_data, at line 55 of FRRouting@@frr-frr-7.2.1-CVE-2023-41361-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_vty_out passes to capability_mp_data, at line 55 of FRRouting@@frr-frr-7.2.1-CVE-2023-41361-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-41361-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-41361-TP.c
Line	78	78
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-41361-TP.c
Method void bgp_capability_vty_out(struct vty *vty, struct peer *peer, bool use_json,

```
....
78.           memcpy(&mpc, pnt + 2, sizeof(struct capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=101
Status	New

The size of the buffer used by bgp_route_refresh_receive in uint32_t, at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to uint32_t, at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	1900	1900
Object	uint32_t	uint32_t

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1900.                                                             sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=102
Status	New

The size of the buffer used by bgp_capability_msg_parse in capability_mp_data, at line 2045 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_msg_parse passes to capability_mp_data, at line 2045 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	2092	2092
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,

```
....
2092.                 memcpy(&mpc, pnt + 3, sizeof(struct
capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=103
Status	New

The size of the buffer used by bgp_route_refresh_receive in uint32_t, at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to uint32_t, at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	1900	1900
Object	uint32_t	uint32_t

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method	static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1900.                                                   sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=104
Status	New

The size of the buffer used by bgp_capability_msg_parse in capability_mp_data, at line 2045 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_msg_parse passes to capability_mp_data, at line 2045 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	2092	2092
Object	capability_mp_data	capability_mp_data

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method	static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,

```
....
2092.              memcpy(&mpc, pnt + 3, sizeof(struct
capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=105
Status	New

The size of the buffer used by really_send_update in ->, at line 1032 of FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1032 of FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c
Line	1100	1100
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c
Method really_send_update(struct interface *ifp,

```
....
1100.          memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=106
Status	New

The size of the buffer used by really_send_update in ->, at line 1032 of FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1032 of FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c
Line	1100	1100
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c
Method really_send_update(struct interface *ifp,

```
....
1100.         memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=107
Status	New

The size of the buffer used by really_send_update in ->, at line 1032 of FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1032 of FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c
Line	1100	1100
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c
Method really_send_update(struct interface *ifp,

```
....
1100.         memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=108
Status	New

The size of the buffer used by bgp_route_refresh_receive in uint32_t, at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to uint32_t, at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	1904	1904
Object	uint32_t	uint32_t

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1904.                                                   sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=109
Status	New

The size of the buffer used by bgp_capability_msg_parse in capability_mp_data, at line 2049 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_msg_parse passes to capability_mp_data, at line 2049 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	2099	2099
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,

```
....
2099.                memcpy(&mpc, pnt + 3, sizeof(struct
capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=110
Status	New

The size of the buffer used by bgp_capability_vty_out in capability_mp_data, at line 55 of FRRouting@@frr-frr-7.3.1-CVE-2023-31489-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_vty_out passes to capability_mp_data, at line 55 of FRRouting@@frr-frr-7.3.1-CVE-2023-31489-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-31489-FP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-31489-FP.c

Line	78	78
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-31489-FP.c
Method void bgp_capability_vty_out(struct vty *vty, struct peer *peer, bool use_json,

```
....
78.          memcpy(&mpc, pnt + 2, sizeof(struct capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=111
Status	New

The size of the buffer used by really_send_update in ->, at line 1032 of FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1032 of FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c
Line	1100	1100
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c
Method really_send_update(struct interface *ifp,

```
....
1100.         memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=112
Status	New

The size of the buffer used by bgp_capability_vty_out in capability_mp_data, at line 55 of FRRouting@@frr-frr-7.3.1-CVE-2023-41361-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_vty_out passes to capability_mp_data, at line 55 of FRRouting@@frr-frr-7.3.1-CVE-2023-41361-TP.c, to overwrite the target buffer.

	Source	Destination

File	FRRouting@@frr-frr-7.3.1-CVE-2023-41361-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-41361-TP.c
Line	78	78
Object	capability_mp_data	capability_mp_data

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-41361-TP.c
Method	void bgp_capability_vty_out(struct vty *vty, struct peer *peer, bool use_json,

```
....
78.          memcpy(&mpc, pnt + 2, sizeof(struct capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=113
Status	New

The size of the buffer used by bgp_route_refresh_receive in uint32_t, at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to uint32_t, at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	1904	1904
Object	uint32_t	uint32_t

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method	static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1904.                                               sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=114
Status	New

The size of the buffer used by bgp_capability_msg_parse in capability_mp_data, at line 2049 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_msg_parse passes to capability_mp_data, at line 2049 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	2099	2099
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,

```
....
2099.                 memcpy(&mpc, pnt + 3, sizeof(struct
capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=115
Status	New

The size of the buffer used by bgp_route_refresh_receive in uint32_t, at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to uint32_t, at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	1904	1904
Object	uint32_t	uint32_t

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1904.                                                      sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=116
Status	New

The size of the buffer used by bgp_capability_msg_parse in capability_mp_data, at line 2049 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_msg_parse passes to capability_mp_data, at line 2049 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	2099	2099
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,

```
....
2099.                memcpy(&mpc, pnt + 3, sizeof(struct
capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=117
Status	New

The size of the buffer used by really_send_update in ->, at line 1031 of FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1031 of FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c
Line	1099	1099
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c
Method really_send_update(struct interface *ifp,

```
....
1099.             memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=118
Status	New

The size of the buffer used by really_send_update in ->, at line 1031 of FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1031 of FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c
Line	1099	1099
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c
Method really_send_update(struct interface *ifp,

```
....
1099.           memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=119
Status	New

The size of the buffer used by really_send_update in ->, at line 1031 of FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1031 of FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c
Line	1099	1099
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c
Method really_send_update(struct interface *ifp,

```
....
1099.           memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=120
Status	New

The size of the buffer used by bgp_route_refresh_receive in uint32_t, at line 1883 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to uint32_t, at line 1883 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	2018	2018
Object	uint32_t	uint32_t

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Method	static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
2018.                                                        sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=121
Status	New

The size of the buffer used by bgp_capability_msg_parse in capability_mp_data, at line 2153 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_msg_parse passes to capability_mp_data, at line 2153 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	2203	2203
Object	capability_mp_data	capability_mp_data

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Method	static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,

```
....
2203.             memcpy(&mpc, pnt + 3, sizeof(struct
capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=122
Status	New

The size of the buffer used by bgp_capability_vty_out in capability_mp_data, at line 55 of FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_vty_out passes to capability_mp_data, at line 55 of FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c
Line	78	78
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c
Method void bgp_capability_vty_out(struct vty *vty, struct peer *peer, bool use_json,

```
....
78.         memcpy(&mpc, pnt + 2, sizeof(struct capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=123
Status	New

The size of the buffer used by bgp_route_refresh_receive in uint32_t, at line 1883 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to uint32_t, at line 1883 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Line	2018	2018
Object	uint32_t	uint32_t

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Method	static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
2018.                                              sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=124
Status	New

The size of the buffer used by bgp_capability_msg_parse in capability_mp_data, at line 2153 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_msg_parse passes to capability_mp_data, at line 2153 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Line	2203	2203
Object	capability_mp_data	capability_mp_data

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Method	static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,

```
....
2203.              memcpy(&mpc, pnt + 3, sizeof(struct
capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=125
Status	New

The size of the buffer used by bgp_route_refresh_receive in uint32_t, at line 1883 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to uint32_t, at line 1883 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Line	2018	2018

Object	uint32_t	uint32_t

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
2018.                                               sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=126
Status	New

The size of the buffer used by bgp_capability_msg_parse in capability_mp_data, at line 2153 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_msg_parse passes to capability_mp_data, at line 2153 of FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Line	2203	2203
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2024-31949-TP.c
Method static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,

```
....
2203.            memcpy(&mpc, pnt + 3, sizeof(struct
capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=127
Status	New

The size of the buffer used by really_send_update in ->, at line 1030 of FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1030 of FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c, to overwrite the target buffer.

	Source	Destination

File	FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c
Line	1098	1098
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c
Method really_send_update(struct interface *ifp,

```
....
1098.           memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=128
Status	New

The size of the buffer used by really_send_update in ->, at line 1030 of FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1030 of FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c
Line	1098	1098
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c
Method really_send_update(struct interface *ifp,

```
....
1098.           memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp-
>buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=129
Status	New

The size of the buffer used by really_send_update in ->, at line 1030 of FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1030 of FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c
Line	1098	1098
Object	->	->

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c
Method really_send_update(struct interface *ifp,

```
....
1098.           memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp->buffered_id));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=130
Status	New

The size of the buffer used by bgp_route_refresh_receive in uint32_t, at line 1933 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to uint32_t, at line 1933 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Line	2092	2092
Object	uint32_t	uint32_t

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
2092.                                                 sizeof(uint32_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=131
Status	New

The size of the buffer used by bgp_capability_msg_parse in capability_mp_data, at line 2350 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_msg_parse passes to capability_mp_data, at line 2350 of FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Line	2400	2400
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2022-37032-TP.c
Method static int bgp_capability_msg_parse(struct peer *peer, uint8_t *pnt,

```
....
2400.                 memcpy(&mpc, pnt + 3, sizeof(struct
capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=132
Status	New

The size of the buffer used by bgp_capability_vty_out in capability_mp_data, at line 55 of FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_capability_vty_out passes to capability_mp_data, at line 55 of FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c
Line	78	78
Object	capability_mp_data	capability_mp_data

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c
Method void bgp_capability_vty_out(struct vty *vty, struct peer *peer, bool use_json,

```
....
78.         memcpy(&mpc, pnt + 2, sizeof(struct capability_mp_data));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=133
Status	New

The size of the buffer used by really_send_update in ->, at line 1030 of FRRouting@@frr-frr-8.0.1-CVE-2023-3748-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that really_send_update passes to ->, at line 1030 of FRRouting@@frr-frr-8.0.1-CVE-2023-3748-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-3748-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-3748-TP.c
Line	1098	1098
Object	->	->

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2023-3748-TP.c
Method	really_send_update(struct interface *ifp,

```
....
1098.          memcpy(babel_ifp->buffered_id, id, sizeof(babel_ifp->buffered_id));
```

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=1000020&projectid=15&pathid=2026
Status	New

The variable declared in li at freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c in line 763 is not initialized when it is used by li at freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c in line 763.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	767	781
Object	li	li

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	char *stun_determine_ip_address(int family)

```
....
767.    su_localinfo_t *li = NULL, hints[1] = {{ LI_CANONNAME|LI_NUMERIC
}};
....
781.    temp = li->li_addr;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2027
Status	New

The variable declared in li at freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c in line 763 is not initialized when it is used by li at freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c in line 763.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	767	781
Object	li	li

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method char *stun_determine_ip_address(int family)

```
....
767.    su_localinfo_t *li = NULL, hints[1] = {{ LI_CANONNAME|LI_NUMERIC
}};
....
781.    temp = li->li_addr;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2028
Status	New

The variable declared in li at freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c in line 763 is not initialized when it is used by li at freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c in line 763.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	767	781
Object	li	li

Code Snippet	
File Name	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method	char *stun_determine_ip_address(int family)

```
....
767.    su_localinfo_t *li = NULL, hints[1] = {{ LI_CANONNAME|LI_NUMERIC
}};
....
781.    temp = li->li_addr;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2029
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by cvt_deltas at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3194.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	3421
Object	mmvar	cvt_deltas

Code Snippet	
File Name	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2045.      FT_MM_Var*          mmvar = NULL;
```

File Name	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method	tt_face_vary_cvt(TT_Face face,

```
....
3421.            cvt_deltas[j] = old_cvt_delta + FT_MulFix( deltas[j],
apply );
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2030
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by cvt_deltas at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3194.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	3463
Object	mmvar	cvt_deltas

Code Snippet
File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3463.             cvt_deltas[pindex] = old_cvt_delta + FT_MulFix(
deltas[j], apply );
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2031
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by cvt at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3194.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	3430
Object	mmvar	cvt

Code Snippet
File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.        FT_MM_Var*           mmvar = NULL;
```

File Name	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method	tt_face_vary_cvt(TT_Face face,

```
....
3430.                               ( FT_fdot6ToFixed( face->cvt[j] ) +
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2032
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by cvt at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3194.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	3472
Object	mmvar	cvt

Code Snippet

File Name	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2045.        FT_MM_Var*           mmvar = NULL;
```

File Name	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method	tt_face_vary_cvt(TT_Face face,

```
....
3472.                               ( FT_fdot6ToFixed( face->cvt[pindex] ) +
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2033
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by mmvar at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	2213
Object	mmvar	mmvar

Code Snippet
File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*             mmvar = NULL;
....
2213.           (FT_UShort*)(  (char*)mmvar + mmvar_size );
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2034
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by cvt_deltas at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3194.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	2045	3421
Object	mmvar	cvt_deltas

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*             mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method tt_face_vary_cvt(TT_Face face,

```
....
3421.              cvt_deltas[j] = old_cvt_delta + FT_MulFix( deltas[j],
apply );
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2035
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by cvt_deltas at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3194.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	2045	3463
Object	mmvar	cvt_deltas

Code Snippet
File Name   freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method   TT_Get_MM_Var(TT_Face   face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name   freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method   tt_face_vary_cvt(TT_Face   face,

```
....
3463.              cvt_deltas[pindex] = old_cvt_delta + FT_MulFix(
deltas[j], apply );
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2036
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by cvt at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3194.

	Source	Destination

File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	2045	3430
Object	mmvar	cvt

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

▼

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3430.                                ( FT_fdot6ToFixed( face->cvt[j] ) +
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2037
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by cvt at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3194.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	2045	3472
Object	mmvar	cvt

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

▼

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3472.                                   ( FT_fdot6ToFixed( face->cvt[pindex] ) +
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2038
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by mmvar at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	2045	2213
Object	mmvar	mmvar

Code Snippet

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2045.      FT_MM_Var*            mmvar = NULL;
....
2213.           (FT_UShort*)( (char*)mmvar + mmvar_size );
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2039
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by cvt_deltas at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3206.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	2056	3433
Object	mmvar	cvt_deltas

Code Snippet

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2056.       FT_MM_Var*            mmvar = NULL;
```

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	tt_face_vary_cvt(TT_Face face,

```
....
3433.            cvt_deltas[j] = old_cvt_delta + FT_MulFix( deltas[j],
apply );
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2040
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by cvt_deltas at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3206.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	2056	3475
Object	mmvar	cvt_deltas

Code Snippet

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2056.       FT_MM_Var*            mmvar = NULL;
```

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	tt_face_vary_cvt(TT_Face face,

```
....
3475.            cvt_deltas[pindex] = old_cvt_delta + FT_MulFix(
deltas[j], apply );
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2041
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by cvt at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3206.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	2056	3442
Object	mmvar	cvt

Code Snippet
File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2056.       FT_MM_Var*            mmvar = NULL;
```

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	tt_face_vary_cvt(TT_Face face,

```
....
3442.                         ( FT_fdot6ToFixed( face->cvt[j] ) +
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2042
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by cvt at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3206.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	2056	3484
Object	mmvar	cvt

Code Snippet
File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2056.      FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3484.                             ( FT_fdot6ToFixed( face->cvt[pindex] ) +
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2043
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by mmvar at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	2056	2224
Object	mmvar	mmvar

Code Snippet

File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2056.      FT_MM_Var*            mmvar = NULL;
....
2224.          (FT_UShort*)( (char*)mmvar + mmvar_size );
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2044
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by cvt_deltas at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3280.

	Source	Destination

File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	2125	3507
Object	mmvar	cvt_deltas

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method tt_face_vary_cvt(TT_Face face,

```
....
3507.             cvt_deltas[j] = old_cvt_delta + FT_MulFix( deltas[j],
apply );
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2045
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by cvt_deltas at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3280.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	2125	3549
Object	mmvar	cvt_deltas

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method tt_face_vary_cvt(TT_Face face,

```
....
3549.           cvt_deltas[pindex] = old_cvt_delta + FT_MulFix(
deltas[j], apply );
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2046
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by cvt at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3280.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	2125	3516
Object	mmvar	cvt

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*          mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3516.                         ( FT_fdot6ToFixed( face->cvt[j] ) +
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2047
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by cvt at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3280.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-	freetype@@freetype-VER-2-11-1-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	2125	3558
Object	mmvar	cvt

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*             mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3558.                           ( FT_fdot6ToFixed( face->cvt[pindex] ) +
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2048
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by mmvar at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	2125	2293
Object	mmvar	mmvar

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*             mmvar = NULL;
....
2293.           (FT_UShort*)( (char*)mmvar + mmvar_size );
```

Use of Zero Initialized Pointer\Path 24:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2049
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by cvt_deltas at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 3271.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	2118	3499
Object	mmvar	cvt_deltas

Code Snippet

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2118.       FT_MM_Var*              mmvar = NULL;
```

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3499.             cvt_deltas[j] = old_cvt_delta + FT_MulFix( deltas[j],
apply );
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2050
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by cvt_deltas at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 3271.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	2118	3541
Object	mmvar	cvt_deltas

Code Snippet

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2118.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3541.             cvt_deltas[pindex] = old_cvt_delta + FT_MulFix(
deltas[j], apply );
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2051
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by cvt at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 3271.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	2118	3508
Object	mmvar	cvt

Code Snippet

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2118.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3508.                          ( FT_fdot6ToFixed( face->cvt[j] ) +
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=2052
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by cvt at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 3271.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	2118	3550
Object	mmvar	cvt

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2118.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method tt_face_vary_cvt(TT_Face face,

```
....
3550.                         ( FT_fdot6ToFixed( face->cvt[pindex] ) +
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2053
Status	New

The variable declared in mmvar at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by mmvar at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	2118	2286
Object	mmvar	mmvar

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2118.        FT_MM_Var*            mmvar = NULL;
....
2286.            (FT_UShort*)( (char*)mmvar + mmvar_size );
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2054
Status	New

The variable declared in successor at FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c in line 1756 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c in line 862.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c
Line	1762	878
Object	successor	unicast_neighbour

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c
Method	handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1762.        struct neighbour *successor = NULL;
```

▼

File Name	FRRouting@@frr-frr-7.2.1-CVE-2022-26127-TP.c
Method	start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
878.        unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2055
Status	New

The variable declared in successor at FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c in line 1756 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c in line 862.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c
Line	1762	878
Object	successor	unicast_neighbour

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c
Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1762.       struct neighbour *successor = NULL;
```

File Name FRRouting@@frr-frr-7.2.1-CVE-2022-26128-TP.c
Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
878.      unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2056
Status	New

The variable declared in successor at FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c in line 1756 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c in line 862.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c
Line	1762	878
Object	successor	unicast_neighbour

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c
Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1762.       struct neighbour *successor = NULL;
```

File Name FRRouting@@frr-frr-7.2.1-CVE-2022-26129-TP.c

Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
878.        unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2057
Status	New

The variable declared in successor at FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c in line 1756 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c in line 862.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c
Line	1762	878
Object	successor	unicast_neighbour

Code Snippet

File Name FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c

Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1762.        struct neighbour *successor = NULL;
```

File Name FRRouting@@frr-frr-7.2.1-CVE-2023-3748-TP.c

Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
878.        unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2058
Status	New

The variable declared in key at FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c in line 163 is not initialized when it is used by key at FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c in line 163.

	Source	Destination

File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	170	214
Object	key	key

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
170.        struct key *key = NULL;
....
214.              MD5Update(&ctx, key->string, strlen(key->string));
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2059
Status	New

The variable declared in key at FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c in line 163 is not initialized when it is used by key at FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c in line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	170	214
Object	key	key

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
170.        struct key *key = NULL;
....
214.              MD5Update(&ctx, key->string, strlen(key->string));
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2060
Status	New

The variable declared in key at FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c in line 163 is not initialized when it is used by key at FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c in line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	170	221
Object	key	key

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
170.        struct key *key = NULL;
....
221.              MD5Update(&ctx, key->string, strlen(key->string));
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2061
Status	New

The variable declared in key at FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c in line 163 is not initialized when it is used by key at FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c in line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	170	221
Object	key	key

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
170.        struct key *key = NULL;
....
221.              MD5Update(&ctx, key->string, strlen(key->string));
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2062
Status	New

The variable declared in successor at FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c in line 1756 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c in line 862.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c
Line	1762	878
Object	successor	unicast_neighbour

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c
Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1762.       struct neighbour *successor = NULL;
```

File Name FRRouting@@frr-frr-7.3.1-CVE-2022-26127-TP.c

Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
878.       unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2063
Status New

The variable declared in successor at FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c in line 1756 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c in line 862.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c
Line	1762	878
Object	successor	unicast_neighbour

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c
Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1762.       struct neighbour *successor = NULL;
```

File Name	FRRouting@@frr-frr-7.3.1-CVE-2022-26128-TP.c
Method	start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
878.       unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2064
Status	New

The variable declared in successor at FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c in line 1756 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c in line 862.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c
Line	1762	878
Object	successor	unicast_neighbour

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c
Method	handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1762.       struct neighbour *successor = NULL;
```

File Name	FRRouting@@frr-frr-7.3.1-CVE-2022-26129-TP.c
Method	start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
878.       unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2065
Status	New

The variable declared in successor at FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c in line 1756 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c in line 862.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c
Line	1762	878
Object	successor	unicast_neighbour

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c
Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1762.       struct neighbour *successor = NULL;
```

File Name FRRouting@@frr-frr-7.3.1-CVE-2023-3748-TP.c
Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
878.       unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2066
Status	New

The variable declared in key at FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c in line 163 is not initialized when it is used by key at FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c in line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	170	214
Object	key	key

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
170.        struct key *key = NULL;
....
214.              MD5Update(&ctx, key->string, strlen(key->string));
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2067
Status	New

The variable declared in key at FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c in line 163 is not initialized when it is used by key at FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c in line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	170	214
Object	key	key

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method	int eigrp_check_md5_digest(struct stream *s,

```
....
170.        struct key *key = NULL;
....
214.              MD5Update(&ctx, key->string, strlen(key->string));
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2068
Status	New

The variable declared in key at FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c in line 163 is not initialized when it is used by key at FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c in line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	170	221
Object	key	key

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method	int eigrp_check_md5_digest(struct stream *s,

```
....
170.        struct key *key = NULL;
....
221.                MD5Update(&ctx, key->string, strlen(key->string));
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2069
Status	New

The variable declared in key at FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c in line 163 is not initialized when it is used by key at FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c in line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	170	221
Object	key	key

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method	int eigrp_check_md5_digest(struct stream *s,

```
....
170.        struct key *key = NULL;
....
221.                MD5Update(&ctx, key->string, strlen(key->string));
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2070
Status	New

The variable declared in successor at FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c in line 1755 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c in line 861.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c
Line	1761	877

Object	successor	unicast_neighbour

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c
Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1761.       struct neighbour *successor = NULL;
```

File Name FRRouting@@frr-frr-7.5.1-CVE-2022-26127-FP.c

Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
877.        unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2071
Status	New

The variable declared in successor at FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c in line 1755 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c in line 861.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c
Line	1761	877
Object	successor	unicast_neighbour

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c
Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1761.       struct neighbour *successor = NULL;
```

File Name FRRouting@@frr-frr-7.5.1-CVE-2022-26128-FP.c

Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
877.        unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2072
Status	New

The variable declared in successor at FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c in line 1755 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c in line 861.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c
Line	1761	877
Object	successor	unicast_neighbour

Code Snippet

File Name FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c

Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1761.        struct neighbour *successor = NULL;
```

File Name FRRouting@@frr-frr-7.5.1-CVE-2022-26129-FP.c

Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
877.        unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2073
Status	New

The variable declared in successor at FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c in line 1754 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c in line 860.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c
Line	1760	876
Object	successor	unicast_neighbour

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c
Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1760.       struct neighbour *successor = NULL;
```

▼

File Name FRRouting@@frr-frr-8.0.1-CVE-2022-26127-TP.c

Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
876.        unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2074
Status	New

The variable declared in successor at FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c in line 1754 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c in line 860.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c
Line	1760	876
Object	successor	unicast_neighbour

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c
Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1760.       struct neighbour *successor = NULL;
```

▼

File Name FRRouting@@frr-frr-8.0.1-CVE-2022-26128-TP.c

Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
876.        unicast_neighbour = neigh;
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2075
Status	New

The variable declared in successor at FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c in line 1754 is not initialized when it is used by unicast_neighbour at FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c in line 860.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c
Line	1760	876
Object	successor	unicast_neighbour

Code Snippet

File Name FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c

Method handle_request(struct neighbour *neigh, const unsigned char *prefix,

```
....
1760.      struct neighbour *successor = NULL;
```

File Name FRRouting@@frr-frr-8.0.1-CVE-2022-26129-TP.c

Method start_unicast_message(struct neighbour *neigh, int type, int len)

```
....
876.      unicast_neighbour = neigh;
```

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=1000020&projectid=15&pathid=1801
Status	New

Calling free() (line 574) on a variable that was not dynamically allocated (line 574) in file freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c may result with a crash.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	600	600

Object	p	p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_free_message(stun_msg_t *msg) {

```
....
600.        free(p);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1802
Status	New

Calling free() (line 574) on a variable that was not dynamically allocated (line 574) in file freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c may result with a crash.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	600	600
Object	p	p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_free_message(stun_msg_t *msg) {

```
....
600.        free(p);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1803
Status	New

Calling free() (line 574) on a variable that was not dynamically allocated (line 574) in file freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c may result with a crash.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	600	600

Object	p	p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method int stun_free_message(stun_msg_t *msg) {

```
....
600.        free(p);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1804
Status	New

Calling free() (line 221) on a variable that was not dynamically allocated (line 221) in file FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c may result with a crash.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	227	227
Object	here	here

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static void clear(struct pid_list **list)

```
....
227.                free(here);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1805
Status	New

Calling free() (line 65) on a variable that was not dynamically allocated (line 65) in file FRRouting@@frr-frr-8.0.1-CVE-2023-46752-TP.c may result with a crash.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-46752-TP.c
Line	136	136

Object	config_str	config_str

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-46752-TP.c
Method int nb_db_transaction_save(const struct nb_transaction *transaction,

```
....
136.                    free(config_str);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1806
Status	New

Calling free() (line 65) on a variable that was not dynamically allocated (line 65) in file FRRouting@@frr-frr-8.4.4-CVE-2023-46752-TP.c may result with a crash.

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-46752-TP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-46752-TP.c
Line	136	136
Object	config_str	config_str

Code Snippet
File Name FRRouting@@frr-frr-8.4.4-CVE-2023-46752-TP.c
Method int nb_db_transaction_save(const struct nb_transaction *transaction,

```
....
136.                    free(config_str);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1807
Status	New

Calling free() (line 1033) on a variable that was not dynamically allocated (line 1033) in file git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c	git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c
Line	1066	1066

Object	buf	buf

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c
Method int fsck_finish(struct fsck_options *options)

```
....
1066.             free(buf);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1808
Status	New

Calling free() (line 225) on a variable that was not dynamically allocated (line 225) in file git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c	git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c
Line	260	260
Object	to_free	to_free

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c
Method void fsck_set_msg_types(struct fsck_options *options, const char *values)

```
....
260.          free(to_free);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1809
Status	New

Calling free() (line 919) on a variable that was not dynamically allocated (line 919) in file git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c	git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c
Line	957	957

Object	name	name

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2020-11008-TP.c
Method static int fsck_gitmodules_fn(const char *var, const char *value, void *vdata)

```
....
957.        free(name);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1810
Status	New

Calling free() (line 1306) on a variable that was not dynamically allocated (line 1306) in file git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	1374	1374
Object	array	array

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1374.        free(array);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1811
Status	New

Calling free() (line 1306) on a variable that was not dynamically allocated (line 1306) in file git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	1375	1375

Object	wdeltaenv	wdeltaenv

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1375.        free(wdeltaenv);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1812
Status	New

Calling free() (line 1463) on a variable that was not dynamically allocated (line 1463) in file git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	1658	1658
Object	wenvblk	wenvblk

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1658.        free(wenvblk);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1813
Status	New

Calling free() (line 1463) on a variable that was not dynamically allocated (line 1463) in file git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	1659	1659

Object	wargs	wargs

Code Snippet

File Name	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1659.        free(wargs);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1814
Status	New

Calling free() (line 2770) on a variable that was not dynamically allocated (line 2770) in file git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	2833	2833
Object	save	save

Code Snippet

File Name	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method	int wmain(int argc, const wchar_t **wargv)

```
....
2833.        free(save);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1815
Status	New

Calling free() (line 2770) on a variable that was not dynamically allocated (line 2770) in file git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	2834	2834

Object	argv	argv

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method int wmain(int argc, const wchar_t **wargv)

```
....
2834.        free(argv);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1816
Status	New

Calling free() (line 1328) on a variable that was not dynamically allocated (line 1328) in file git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	1396	1396
Object	array	array

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1396.        free(array);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1817
Status	New

Calling free() (line 1328) on a variable that was not dynamically allocated (line 1328) in file git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	1397	1397

Object	wdeltaenv	wdeltaenv

Code Snippet	
File Name	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method	static wchar_t *make_environment_block(char **deltaenv)

```
....
1397.        free(wdeltaenv);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1818
Status	New

Calling free() (line 1485) on a variable that was not dynamically allocated (line 1485) in file git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	1706	1706
Object	wenvblk	wenvblk

Code Snippet	
File Name	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1706.        free(wenvblk);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1819
Status	New

Calling free() (line 1485) on a variable that was not dynamically allocated (line 1485) in file git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	1707	1707

Object	wargs	wargs

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1707.        free(wargs);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1820
Status	New

Calling free() (line 2820) on a variable that was not dynamically allocated (line 2820) in file git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	2883	2883
Object	save	save

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method int wmain(int argc, const wchar_t **wargv)

```
....
2883.        free(save);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1821
Status	New

Calling free() (line 2820) on a variable that was not dynamically allocated (line 2820) in file git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	2884	2884

Object	argv	argv

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method int wmain(int argc, const wchar_t **wargv)

```
....
2884.       free(argv);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1822
Status	New

Calling free() (line 1331) on a variable that was not dynamically allocated (line 1331) in file git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	1399	1399
Object	array	array

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1399.       free(array);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1823
Status	New

Calling free() (line 1331) on a variable that was not dynamically allocated (line 1331) in file git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	1400	1400

Object	wdeltaenv	wdeltaenv

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1400.         free(wdeltaenv);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1824
Status	New

Calling free() (line 1488) on a variable that was not dynamically allocated (line 1488) in file git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	1709	1709
Object	wenvblk	wenvblk

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1709.         free(wenvblk);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1825
Status	New

Calling free() (line 1488) on a variable that was not dynamically allocated (line 1488) in file git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	1710	1710

Object	wargs	wargs

Code Snippet

File Name	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1710.       free(wargs);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1826
Status	New

Calling free() (line 2823) on a variable that was not dynamically allocated (line 2823) in file git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	2886	2886
Object	save	save

Code Snippet

File Name	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method	int wmain(int argc, const wchar_t **wargv)

```
....
2886.       free(save);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1827
Status	New

Calling free() (line 2823) on a variable that was not dynamically allocated (line 2823) in file git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	2887	2887

Object	argv	argv

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method int wmain(int argc, const wchar_t **wargv)

```
....
2887.        free(argv);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1828
Status	New

Calling free() (line 1331) on a variable that was not dynamically allocated (line 1331) in file git@@git-v2.30.1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	1399	1399
Object	array	array

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1399.        free(array);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1829
Status	New

Calling free() (line 1331) on a variable that was not dynamically allocated (line 1331) in file git@@git-v2.30.1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	1400	1400
Object	wdeltaenv	wdeltaenv

Code Snippet

File Name	git@@git-v2.30.1-CVE-2021-21300-TP.c
Method	static wchar_t *make_environment_block(char **deltaenv)

```
....
1400.        free(wdeltaenv);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1830
Status	New

Calling free() (line 1488) on a variable that was not dynamically allocated (line 1488) in file git@@git-v2.30.1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	1709	1709
Object	wenvblk	wenvblk

Code Snippet

File Name	git@@git-v2.30.1-CVE-2021-21300-TP.c
Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1709.        free(wenvblk);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1831
Status	New

Calling free() (line 1488) on a variable that was not dynamically allocated (line 1488) in file git@@git-v2.30.1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	1710	1710
Object	wargs	wargs

Code Snippet

File Name	git@@git-v2.30.1-CVE-2021-21300-TP.c

Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1710.        free(wargs);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1832
Status	New

Calling free() (line 2823) on a variable that was not dynamically allocated (line 2823) in file git@@git-v2.30.1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	2886	2886
Object	save	save

Code Snippet

File Name	git@@git-v2.30.1-CVE-2021-21300-TP.c
Method	int wmain(int argc, const wchar_t **wargv)

```
....
2886.        free(save);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1833
Status	New

Calling free() (line 2823) on a variable that was not dynamically allocated (line 2823) in file git@@git-v2.30.1-CVE-2021-21300-TP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	2887	2887
Object	argv	argv

Code Snippet

File Name	git@@git-v2.30.1-CVE-2021-21300-TP.c
Method	int wmain(int argc, const wchar_t **wargv)

```
....
2887.        free(argv);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1834
Status	New

Calling free() (line 1336) on a variable that was not dynamically allocated (line 1336) in file git@@git-v2.30.3-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	1404	1404
Object	array	array

Code Snippet

File Name git@@git-v2.30.3-CVE-2021-21300-FP.c

Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1404.        free(array);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1835
Status	New

Calling free() (line 1336) on a variable that was not dynamically allocated (line 1336) in file git@@git-v2.30.3-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	1405	1405
Object	wdeltaenv	wdeltaenv

Code Snippet

File Name git@@git-v2.30.3-CVE-2021-21300-FP.c

Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1405.       free(wdeltaenv);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1836
Status	New

Calling free() (line 1493) on a variable that was not dynamically allocated (line 1493) in file git@@git-v2.30.3-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	1714	1714
Object	wenvblk	wenvblk

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1714.       free(wenvblk);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1837
Status	New

Calling free() (line 1493) on a variable that was not dynamically allocated (line 1493) in file git@@git-v2.30.3-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	1715	1715
Object	wargs	wargs

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1715.       free(wargs);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1838
Status	New

Calling free() (line 2914) on a variable that was not dynamically allocated (line 2914) in file git@@git-v2.30.3-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	2977	2977
Object	save	save

Code Snippet

File Name	git@@git-v2.30.3-CVE-2021-21300-FP.c
Method	int wmain(int argc, const wchar_t **wargv)

```
....
2977.       free(save);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1839
Status	New

Calling free() (line 2914) on a variable that was not dynamically allocated (line 2914) in file git@@git-v2.30.3-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	2978	2978
Object	argv	argv

Code Snippet

File Name	git@@git-v2.30.3-CVE-2021-21300-FP.c
Method	int wmain(int argc, const wchar_t **wargv)

```
....
2978.        free(argv);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1840
Status	New

Calling free() (line 1336) on a variable that was not dynamically allocated (line 1336) in file git@@git-v2.30.8-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	1404	1404
Object	array	array

Code Snippet

File Name git@@git-v2.30.8-CVE-2021-21300-FP.c

Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1404.        free(array);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1841
Status	New

Calling free() (line 1336) on a variable that was not dynamically allocated (line 1336) in file git@@git-v2.30.8-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	1405	1405
Object	wdeltaenv	wdeltaenv

Code Snippet

File Name git@@git-v2.30.8-CVE-2021-21300-FP.c

Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1405.       free(wdeltaenv);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1842
Status	New

Calling free() (line 1493) on a variable that was not dynamically allocated (line 1493) in file git@@git-v2.30.8-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	1714	1714
Object	wenvblk	wenvblk

Code Snippet

File Name	git@@git-v2.30.8-CVE-2021-21300-FP.c
Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1714.       free(wenvblk);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1843
Status	New

Calling free() (line 1493) on a variable that was not dynamically allocated (line 1493) in file git@@git-v2.30.8-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	1715	1715
Object	wargs	wargs

Code Snippet

File Name	git@@git-v2.30.8-CVE-2021-21300-FP.c
Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1715.        free(wargs);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1844
Status	New

Calling free() (line 2914) on a variable that was not dynamically allocated (line 2914) in file git@@git-v2.30.8-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	2977	2977
Object	save	save

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method int wmain(int argc, const wchar_t **wargv)

```
....
2977.        free(save);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1845
Status	New

Calling free() (line 2914) on a variable that was not dynamically allocated (line 2914) in file git@@git-v2.30.8-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	2978	2978
Object	argv	argv

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method int wmain(int argc, const wchar_t **wargv)

```
....
2978.        free(argv);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1846
Status	New

Calling free() (line 1335) on a variable that was not dynamically allocated (line 1335) in file git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	1403	1403
Object	array	array

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1403.        free(array);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1847
Status	New

Calling free() (line 1335) on a variable that was not dynamically allocated (line 1335) in file git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	1404	1404
Object	wdeltaenv	wdeltaenv

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method static wchar_t *make_environment_block(char **deltaenv)

```
....
1404.        free(wdeltaenv);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1848
Status	New

Calling free() (line 1492) on a variable that was not dynamically allocated (line 1492) in file git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	1713	1713
Object	wenvblk	wenvblk

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1713.        free(wenvblk);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1849
Status	New

Calling free() (line 1492) on a variable that was not dynamically allocated (line 1492) in file git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	1714	1714
Object	wargs	wargs

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c

Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1714.        free(wargs);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1850
Status	New

Calling free() (line 2827) on a variable that was not dynamically allocated (line 2827) in file git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c may result with a crash.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	2890	2890
Object	save	save

Code Snippet	
File Name	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method	int wmain(int argc, const wchar_t **wargv)

```
....
2890.        free(save);
```

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=1000020&projectid=15&pathid=3291
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	1356	1356

Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method struct TLV_Sequence_Type *eigrp_SequenceTLV_new(void)

```
....
1356.       struct TLV_Sequence_Type *new;
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3292
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	796	796
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method struct eigrp_fifo *eigrp_fifo_new(void)

```
....
796.        struct eigrp_fifo *new;
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3293
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	834	834
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method struct eigrp_packet *eigrp_packet_new(size_t size, struct eigrp_neighbor *nbr)

```
....
834.        struct eigrp_packet *new;
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3294
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	1096	1096
Object	neW	neW

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method	struct eigrp_packet *eigrp_packet_duplicate(struct eigrp_packet *old,

```
....
1096.       struct eigrp_packet *new;
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3295
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	1110	1110
Object	neW	neW

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method	static struct TLV_IPv4_Internal_type *eigrp_IPv4_InternalTLV_new(void)

```
....
1110.       struct TLV_IPv4_Internal_type *new;
```

Memory Leak\Path 6:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3296
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	1320	1320
Object	neW	neW

Code Snippet

File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c

Method struct TLV_MD5_Authentication_Type *eigrp_authTLV_MD5_new(void)

```
....
1320.        struct TLV_MD5_Authentication_Type *new;
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3297
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	1335	1335
Object	neW	neW

Code Snippet

File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c

Method struct TLV_SHA256_Authentication_Type *eigrp_authTLV_SHA256_new(void)

```
....
1335.        struct TLV_SHA256_Authentication_Type *new;
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3298
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46753-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46753-TP.c
Line	207	207
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46753-TP.c
Method struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
207.        struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3299
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46753-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46753-TP.c
Line	725	725
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46753-TP.c
Method struct attr *bgp_attr_aggregate_intern(struct bgp *bgp, uint8_t origin,

```
....
725.        struct attr *new;
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3300
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-47235-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47235-TP.c
Line	207	207

Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47235-TP.c
Method struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
207.        struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3301
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-47235-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47235-TP.c
Line	725	725
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47235-TP.c
Method struct attr *bgp_attr_aggregate_intern(struct bgp *bgp, uint8_t origin,

```
....
725.        struct attr *new;
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3302
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2024-31948-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31948-TP.c
Line	207	207
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2024-31948-TP.c

Method	struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
207.         struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3303
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2024-31948-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31948-TP.c
Line	725	725
Object	neW	neW

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2024-31948-TP.c
Method	struct attr *bgp_attr_aggregate_intern(struct bgp *bgp, uint8_t origin,

```
....
725.         struct attr *new;
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3304
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	1356	1356
Object	neW	neW

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method	struct TLV_Sequence_Type *eigrp_SequenceTLV_new(void)

```
....
1356.        struct TLV_Sequence_Type *new;
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3305
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	796	796
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method struct eigrp_fifo *eigrp_fifo_new(void)

```
....
796.        struct eigrp_fifo *new;
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3306
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	834	834
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method struct eigrp_packet *eigrp_packet_new(size_t size, struct eigrp_neighbor *nbr)

```
....
834.        struct eigrp_packet *new;
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3307
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	1096	1096
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method struct eigrp_packet *eigrp_packet_duplicate(struct eigrp_packet *old,

```
....
1096.        struct eigrp_packet *new;
```

Memory Leak\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3308
Status New

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	1110	1110
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method static struct TLV_IPv4_Internal_type *eigrp_IPv4_InternalTLV_new(void)

```
....
1110.        struct TLV_IPv4_Internal_type *new;
```

Memory Leak\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3309
Status New

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	1320	1320

Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method struct TLV_MD5_Authentication_Type *eigrp_authTLV_MD5_new(void)

```
....
1320.       struct TLV_MD5_Authentication_Type *new;
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3310
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	1335	1335
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method struct TLV_SHA256_Authentication_Type *eigrp_authTLV_SHA256_new(void)

```
....
1335.       struct TLV_SHA256_Authentication_Type *new;
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3311
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46753-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46753-FP.c
Line	219	219
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46753-FP.c
Method struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
219.        struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3312
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46753-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46753-FP.c
Line	932	932
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46753-FP.c
Method struct attr *bgp_attr_aggregate_intern(

```
....
932.        struct attr *new;
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3313
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2024-31948-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2024-31948-TP.c
Line	219	219
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2024-31948-TP.c
Method struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
219.        struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3314
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2024-31948-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2024-31948-TP.c
Line	932	932
Object	neW	neW

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2024-31948-TP.c
Method	struct attr *bgp_attr_aggregate_intern(

```
....
932.        struct attr *new;
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3315
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-46753-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-46753-TP.c
Line	219	219
Object	neW	neW

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2023-46753-TP.c
Method	struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
219.        struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3316
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-46753-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-46753-TP.c
Line	958	958
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-46753-TP.c
Method struct attr *bgp_attr_aggregate_intern(

```
....
958.        struct attr *new;
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3317
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-47235-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-47235-TP.c
Line	219	219
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-47235-TP.c
Method struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
219.        struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3318
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-47235-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-47235-TP.c

Line	958	958
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-47235-TP.c
Method struct attr *bgp_attr_aggregate_intern(

```
....
958.         struct attr *new;
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3319
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2024-31948-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2024-31948-TP.c
Line	219	219
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2024-31948-TP.c
Method struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
219.         struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3320
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2024-31948-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2024-31948-TP.c
Line	958	958
Object	neW	neW

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2024-31948-TP.c
Method	struct attr *bgp_attr_aggregate_intern(

```
....
958.        struct attr *new;
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3321
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-46753-TP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-46753-TP.c
Line	217	217
Object	neW	neW

Code Snippet

File Name	FRRouting@@frr-frr-8.4.4-CVE-2023-46753-TP.c
Method	struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
217.        struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3322
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-46753-TP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-46753-TP.c
Line	985	985
Object	neW	neW

Code Snippet

File Name	FRRouting@@frr-frr-8.4.4-CVE-2023-46753-TP.c
Method	struct attr *bgp_attr_aggregate_intern(

```
....
985.        struct attr *new;
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3323
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-47235-TP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-47235-TP.c
Line	217	217
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-8.4.4-CVE-2023-47235-TP.c
Method struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
217.        struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3324
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-47235-TP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-47235-TP.c
Line	985	985
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-8.4.4-CVE-2023-47235-TP.c
Method struct attr *bgp_attr_aggregate_intern(

```
....
985.        struct attr *new;
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=3325
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2024-31948-TP.c	FRRouting@@frr-frr-8.4.4-CVE-2024-31948-TP.c
Line	217	217
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-8.4.4-CVE-2024-31948-TP.c
Method struct bgp_attr_encap_subtlv *encap_tlv_dup(struct bgp_attr_encap_subtlv *orig)

```
....
217.        struct bgp_attr_encap_subtlv *new;
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3326
Status	New

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2024-31948-TP.c	FRRouting@@frr-frr-8.4.4-CVE-2024-31948-TP.c
Line	985	985
Object	neW	neW

Code Snippet
File Name FRRouting@@frr-frr-8.4.4-CVE-2024-31948-TP.c
Method struct attr *bgp_attr_aggregate_intern(

```
....
985.        struct attr *new;
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3327
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.12-	github@@cmark-gfm-0.29.0.gfm.12-

	CVE-2023-24824-FP.c	CVE-2023-24824-FP.c
Line	380	380
Object	alignments	alignments

Code Snippet
File Name github@@cmark-gfm-0.29.0.gfm.12-CVE-2023-24824-FP.c
Method static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
380.     uint8_t *alignments =
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3328
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-24824-TP.c	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-24824-TP.c
Line	496	496
Object	text	text

Code Snippet
File Name github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-24824-TP.c
Method static void process_footnotes(cmark_parser *parser) {

```
....
496.           cmark_node *text = (cmark_node *)parser->mem->calloc(1,
sizeof(*text));
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3329
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c
Line	284	284
Object	alignments	alignments

Code Snippet

File Name	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c
Method	static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
284.     uint8_t *alignments =
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3330
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-24824-TP.c	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-24824-TP.c
Line	504	504
Object	text	text

Code Snippet

File Name	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-24824-TP.c
Method	static void process_footnotes(cmark_parser *parser) {

```
....
504.            cmark_node *text = (cmark_node *)parser->mem->calloc(1,
sizeof(*text));
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3331
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c
Line	304	304
Object	alignments	alignments

Code Snippet

File Name	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c
Method	static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
304.    uint8_t *alignments =
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3332
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-24824-TP.c	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-24824-TP.c
Line	504	504
Object	text	text

Code Snippet

File Name	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-24824-TP.c
Method	static void process_footnotes(cmark_parser *parser) {

```
....
504.          cmark_node *text = (cmark_node *)parser->mem->calloc(1,
sizeof(*text));
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3333
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c
Line	304	304
Object	alignments	alignments

Code Snippet

File Name	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c
Method	static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
304.    uint8_t *alignments =
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3334
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.7-CVE-2023-24824-TP.c	github@@cmark-gfm-0.29.0.gfm.7-CVE-2023-24824-TP.c
Line	331	331
Object	alignments	alignments

Code Snippet
File Name github@@cmark-gfm-0.29.0.gfm.7-CVE-2023-24824-TP.c
Method static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
331.     uint8_t *alignments =
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3335
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.7-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.7-CVE-2023-37463-TP.c
Line	331	331
Object	alignments	alignments

Code Snippet
File Name github@@cmark-gfm-0.29.0.gfm.7-CVE-2023-37463-TP.c
Method static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
331.     uint8_t *alignments =
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3336
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	181	181
Object	data	data

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_parse_attribute(stun_msg_t *msg, unsigned char *p)

```
....
181.        attr->enc_buf.data = (unsigned char *) malloc(len);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3337
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	246	246
Object	phrase	phrase

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_parse_attr_error_code(stun_attr_t *attr, const unsigned char *p, unsigned len) {

```
....
246.      error->phrase = (char *) malloc(len-3);
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3338
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	317	317

Object	data	data

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_copy_buffer(stun_buffer_t *p, stun_buffer_t *p2) {

```
....
317.     p->data = (unsigned char *) malloc(p->size);
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3339
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	481	481
Object	data	data

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_type_len(stun_attr_t *attr, uint16_t len) {

```
....
481.     attr->enc_buf.data = (unsigned char *) malloc(len + 4);
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3340
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	786	786
Object	local_ip_address	local_ip_address

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method char *stun_determine_ip_address(int family)

```
....
786.     local_ip_address = malloc(address_size + 1);
```

Environment Injection

Query Path:
CPP\Cx\CPP Medium Threat\Environment Injection Version:0

Categories

OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Environment Injection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1948
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	2502	2505
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static void setup_windows_environment(void)

```
....
2502.            if (!(tmp = getenv("TMP")))
....
2505.                setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1949
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	2503	2505

Object	getenv	setenv

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static void setup_windows_environment(void)

```
....
2503.                   tmp = getenv("TEMP");
....
2505.                   setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1950
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	2544	2545
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static void setup_windows_environment(void)

```
....
2544.              if (!tmp && (tmp = getenv("USERPROFILE")))
2545.                   setenv("HOME", tmp, 1);
```

Environment Injection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1951
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	2550	2553
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method	static void setup_windows_environment(void)

```
....
2550.                 if (!(tmp = getenv("TMP")))
....
2553.                       setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1952
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	2551	2553
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method	static void setup_windows_environment(void)

```
....
2551.                       tmp = getenv("TEMP");
....
2553.                       setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1953
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	2592	2593
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method	static void setup_windows_environment(void)

```
....
2592.             if (!tmp && (tmp = getenv("USERPROFILE")))
2593.                   setenv("HOME", tmp, 1);
```

Environment Injection\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1954
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	2553	2556
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method static void setup_windows_environment(void)

```
....
2553.             if (!(tmp = getenv("TMP")))
....
2556.                   setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1955
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	2554	2556
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method static void setup_windows_environment(void)

```
....
2554.                    tmp = getenv("TEMP");
....
2556.                    setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1956
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	2595	2596
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method	static void setup_windows_environment(void)

```
....
2595.               if (!tmp && (tmp = getenv("USERPROFILE")))
2596.                    setenv("HOME", tmp, 1);
```

Environment Injection\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1957
Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	2553	2556
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.30.1-CVE-2021-21300-TP.c
Method	static void setup_windows_environment(void)

```
....
2553.               if (!(tmp = getenv("TMP")))
....
2556.                    setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1958
Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	2554	2556
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method static void setup_windows_environment(void)

```
....
2554.                   tmp = getenv("TEMP");
....
2556.                   setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1959
Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	2595	2596
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method static void setup_windows_environment(void)

```
....
2595.           if (!tmp && (tmp = getenv("USERPROFILE")))
2596.                   setenv("HOME", tmp, 1);
```

Environment Injection\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=1960
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	2558	2561
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2558.                   if (!(tmp = getenv("TMP")))
....
2561.                         setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1961
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	2559	2561
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2559.                         tmp = getenv("TEMP");
....
2561.                         setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1962
Status	New

	Source	Destination

File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	2600	2601
Object	getenv	setenv

Code Snippet
File Name   git@@git-v2.30.3-CVE-2021-21300-FP.c
Method   static void setup_windows_environment(void)

```
....
2600.            if (!tmp && (tmp = getenv("USERPROFILE")))
2601.                setenv("HOME", tmp, 1);
```

Environment Injection\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1963
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	2558	2561
Object	getenv	setenv

Code Snippet
File Name   git@@git-v2.30.8-CVE-2021-21300-FP.c
Method   static void setup_windows_environment(void)

```
....
2558.            if (!(tmp = getenv("TMP")))
....
2561.                setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1964
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	2559	2561
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2559.                         tmp = getenv("TEMP");
....
2561.                         setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1965
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	2600	2601
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2600.                   if (!tmp && (tmp = getenv("USERPROFILE")))
2601.                         setenv("HOME", tmp, 1);
```

Environment Injection\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1966
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	2557	2560
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2557.               if (!(tmp = getenv("TMP")))
....
2560.                       setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1967
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	2558	2560
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2558.                       tmp = getenv("TEMP");
....
2560.                       setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1968
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	2599	2600
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2599.               if (!tmp && (tmp = getenv("USERPROFILE")))
2600.                     setenv("HOME", tmp, 1);
```

Environment Injection\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1969
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	2578	2581
Object	getenv	setenv

Code Snippet

File Name git@@git-v2.33.0-CVE-2021-21300-FP.c

Method static void setup_windows_environment(void)

```
....
2578.               if (!(tmp = getenv("TMP"))) 
....
2581.                     setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1970
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	2579	2581
Object	getenv	setenv

Code Snippet

File Name git@@git-v2.33.0-CVE-2021-21300-FP.c

Method static void setup_windows_environment(void)

```
....
2579.                     tmp = getenv("TEMP");
....
2581.                     setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1971
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	2620	2621
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.33.0-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2620.                 if (!tmp && (tmp = getenv("USERPROFILE")))
2621.                       setenv("HOME", tmp, 1);
```

Environment Injection\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1972
Status	New

	Source	Destination
File	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	2578	2581
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.34.1-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2578.                 if (!(tmp = getenv("TMP")))
....
2581.                       setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1973

Status	New

	Source	Destination
File	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	2579	2581
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.34.1-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2579.                        tmp = getenv("TEMP");
....
2581.                        setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1974
Status	New

	Source	Destination
File	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	2620	2621
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.34.1-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2620.                  if (!tmp && (tmp = getenv("USERPROFILE")))
2621.                        setenv("HOME", tmp, 1);
```

Environment Injection\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1975
Status	New

	Source	Destination
File	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c

Line	2602	2605
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.37.0-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2602.                 if (!(tmp = getenv("TMP")))
....
2605.                       setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1976
Status	New

	Source	Destination
File	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	2603	2605
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.37.0-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2603.                       tmp = getenv("TEMP");
....
2605.                       setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1977
Status	New

	Source	Destination
File	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	2644	2645
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.37.0-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2644.              if (!tmp && (tmp = getenv("USERPROFILE")))
2645.                   setenv("HOME", tmp, 1);
```

Environment Injection\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1978
Status	New

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	2600	2603
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2600.              if (!(tmp = getenv("TMP")))
....
2603.                   setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1979
Status	New

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	2601	2603
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2601.           tmp = getenv("TEMP");
....
2603.           setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1980
Status	New

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	2642	2643
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2642.       if (!tmp && (tmp = getenv("USERPROFILE")))
2643.           setenv("HOME", tmp, 1);
```

Environment Injection\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1981
Status	New

	Source	Destination
File	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	2603	2606
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.39.5-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2603.       if (!(tmp = getenv("TMP")))
....
2606.           setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1982
Status	New

	Source	Destination
File	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	2604	2606
Object	getenv	setenv

Code Snippet

File Name git@@git-v2.39.5-CVE-2021-21300-FP.c

Method static void setup_windows_environment(void)

```
....
2604.                        tmp = getenv("TEMP");
....
2606.                        setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1983
Status	New

	Source	Destination
File	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	2645	2646
Object	getenv	setenv

Code Snippet

File Name git@@git-v2.39.5-CVE-2021-21300-FP.c

Method static void setup_windows_environment(void)

```
....
2645.                  if (!tmp && (tmp = getenv("USERPROFILE")))
2646.                        setenv("HOME", tmp, 1);
```

Environment Injection\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=1984
Status	New

	Source	Destination
File	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	2606	2609
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2606.                 if (!(tmp = getenv("TMP")))
....
2609.                       setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1985
Status	New

	Source	Destination
File	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	2607	2609
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2607.                       tmp = getenv("TEMP");
....
2609.                       setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1986
Status	New

	Source	Destination
File	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	2648	2649
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2648.               if (!tmp && (tmp = getenv("USERPROFILE")))
2649.                      setenv("HOME", tmp, 1);
```

Environment Injection\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1987
Status	New

	Source	Destination
File	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	2611	2614
Object	getenv	setenv

Code Snippet
File Name git@@git-v2.42.0-CVE-2021-21300-FP.c
Method static void setup_windows_environment(void)

```
....
2611.               if (!(tmp = getenv("TMP")))
....
2614.                      setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1988
Status	New

	Source	Destination
File	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	2612	2614

Object	getenv	setenv

Code Snippet
File Name	git@@git-v2.42.0-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2612.                   tmp = getenv("TEMP");
....
2614.                   setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1989
Status	New

	Source	Destination
File	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	2653	2654
Object	getenv	setenv

Code Snippet
File Name	git@@git-v2.42.0-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2653.              if (!tmp && (tmp = getenv("USERPROFILE")))
2654.                   setenv("HOME", tmp, 1);
```

Environment Injection\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1990
Status	New

	Source	Destination
File	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	2613	2616
Object	getenv	setenv

Code Snippet
File Name	git@@git-v2.43.1-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2613.            if (!(tmp = getenv("TMP")))
....
2616.                    setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1991
Status	New

	Source	Destination
File	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	2614	2616
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.43.1-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2614.                    tmp = getenv("TEMP");
....
2616.                    setenv("TMPDIR", tmp, 1);
```

Environment Injection\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1992
Status	New

	Source	Destination
File	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	2655	2656
Object	getenv	setenv

Code Snippet

File Name	git@@git-v2.43.1-CVE-2021-21300-FP.c
Method	static void setup_windows_environment(void)

```
....
2655.            if (!tmp && (tmp = getenv("USERPROFILE")))
2656.                    setenv("HOME", tmp, 1);
```

Stored Buffer Overflow boundcpy

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow boundcpy Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Stored Buffer Overflow boundcpy\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2279
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2280
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that credential_read passes to buf, at line 346 of git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

▼

File Name git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2281
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

▼

File Name git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2282
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet

File Name git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2283
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that credential_read passes to buf, at line 346 of git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2284
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2285
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet

File Name	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2286
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that credential_read passes to buf, at line 346 of git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2287
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2288
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.30.1-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.30.1-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.1-CVE-2020-5260-FP.c	git@@git-v2.30.1-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet

File Name	git@@git-v2.30.1-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.30.1-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2289
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.30.1-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.30.1-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.1-CVE-2020-5260-FP.c	git@@git-v2.30.1-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet
File Name git@@git-v2.30.1-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.30.1-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.         memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2290
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.30.1-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.30.1-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.1-CVE-2020-5260-FP.c	git@@git-v2.30.1-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet
File Name git@@git-v2.30.1-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.30.1-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2291
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.30.3-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.30.3-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.3-CVE-2020-5260-FP.c	git@@git-v2.30.3-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet

File Name git@@git-v2.30.3-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.30.3-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2292
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.30.3-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.30.3-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.3-CVE-2020-5260-FP.c	git@@git-v2.30.3-CVE-2020-5260-FP.c

Line	355	332
Object	buf	c

Code Snippet
File Name git@@git-v2.30.3-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.30.3-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2293
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.30.3-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.30.3-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.3-CVE-2020-5260-FP.c	git@@git-v2.30.3-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet
File Name git@@git-v2.30.3-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.30.3-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2294
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.30.8-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.30.8-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.8-CVE-2020-5260-FP.c	git@@git-v2.30.8-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet

File Name git@@git-v2.30.8-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.30.8-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2295
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.30.8-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.30.8-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.8-CVE-2020-5260-FP.c	git@@git-v2.30.8-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet

File Name	git@@git-v2.30.8-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.30.8-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.         memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2296
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.30.8-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.30.8-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.30.8-CVE-2020-5260-FP.c	git@@git-v2.30.8-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet

File Name	git@@git-v2.30.8-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.30.8-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.         memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 19:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2297
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet

File Name	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2298
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet

File Name	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

▼

File Name	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2299
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet

File Name	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

▼

File Name	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 22:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2300
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.33.0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.33.0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.33.0-CVE-2020-5260-FP.c	git@@git-v2.33.0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet

File Name git@@git-v2.33.0-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.33.0-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2301
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.33.0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.33.0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.33.0-CVE-2020-5260-FP.c	git@@git-v2.33.0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet

File Name git@@git-v2.33.0-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.          while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.33.0-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.          memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2302
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.33.0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.33.0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.33.0-CVE-2020-5260-FP.c	git@@git-v2.33.0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet

File Name git@@git-v2.33.0-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.          while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.33.0-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.          memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2303
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.34.1-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.34.1-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.34.1-CVE-2020-5260-FP.c	git@@git-v2.34.1-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet
File Name git@@git-v2.34.1-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.34.1-CVE-2020-5260-FP.c
Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2304
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.34.1-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.34.1-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.34.1-CVE-2020-5260-FP.c	git@@git-v2.34.1-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet
File Name git@@git-v2.34.1-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.34.1-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.         memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2305
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.34.1-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.34.1-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.34.1-CVE-2020-5260-FP.c	git@@git-v2.34.1-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet

File Name	git@@git-v2.34.1-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.34.1-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.         memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2306
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.37.0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.37.0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.37.0-CVE-2020-5260-FP.c	git@@git-v2.37.0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet
File Name	git@@git-v2.37.0-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.		while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.37.0-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.		memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2307
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.37.0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.37.0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.37.0-CVE-2020-5260-FP.c	git@@git-v2.37.0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet
File Name	git@@git-v2.37.0-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.		while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.37.0-CVE-2020-5260-FP.c

Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2308
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.37.0-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.37.0-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.37.0-CVE-2020-5260-FP.c	git@@git-v2.37.0-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet

File Name	git@@git-v2.37.0-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name	git@@git-v2.37.0-CVE-2020-5260-FP.c
Method	static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2309
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination

File	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet
File Name git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.         memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2310
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet
File Name git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2311
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet

File Name git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

▼

File Name git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2312
Status	New

The size of the buffer used by credential_init in Pointer, at line 330 of git@@git-v2.39.5-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.39.5-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination

File	git@@git-v2.39.5-CVE-2020-5260-FP.c	git@@git-v2.39.5-CVE-2020-5260-FP.c
Line	355	332
Object	buf	Pointer

Code Snippet

File Name git@@git-v2.39.5-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.39.5-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2313
Status	New

The size of the buffer used by credential_init in c, at line 330 of git@@git-v2.39.5-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.39.5-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.39.5-CVE-2020-5260-FP.c	git@@git-v2.39.5-CVE-2020-5260-FP.c
Line	355	332
Object	buf	c

Code Snippet

File Name git@@git-v2.39.5-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.39.5-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

Stored Buffer Overflow boundcpy\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2314
Status	New

The size of the buffer used by credential_init in sizeof, at line 330 of git@@git-v2.39.5-CVE-2020-5260-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that credential_read passes to buf, at line 346 of git@@git-v2.39.5-CVE-2020-5260-FP.c, to overwrite the target buffer.

	Source	Destination
File	git@@git-v2.39.5-CVE-2020-5260-FP.c	git@@git-v2.39.5-CVE-2020-5260-FP.c
Line	355	332
Object	buf	sizeof

Code Snippet
File Name git@@git-v2.39.5-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

File Name git@@git-v2.39.5-CVE-2020-5260-FP.c

Method static void credential_init(struct credential *c)

```
....
332.        memset(c, 0, sizeof(*c));
```

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=1000020&projectid=15&pathid=381
Status	New

The function len in git@@git-v2.30.3-CVE-2021-21300-FP.c at line 2605 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	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	2618	2618
Object	len	len

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2618.                   result = xmalloc(len);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=382
Status	New

The function len in git@@git-v2.30.8-CVE-2021-21300-FP.c at line 2605 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	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	2618	2618
Object	len	len

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2618.                   result = xmalloc(len);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=383
Status	New

The function len in git@@git-v2.37.0-CVE-2021-21300-FP.c at line 2649 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	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	2662	2662
Object	len	len

Code Snippet
File Name git@@git-v2.37.0-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2662.                    result = xmalloc(len);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=384
Status	New

The function len in git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c at line 2647 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	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	2660	2660
Object	len	len

Code Snippet
File Name git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2660.                    result = xmalloc(len);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=385
Status	New

The function len in git@@git-v2.39.5-CVE-2021-21300-FP.c at line 2650 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	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	2663	2663
Object	len	len

Code Snippet

File Name	git@@git-v2.39.5-CVE-2021-21300-FP.c
Method	static PSID get_current_user_sid(void)

```
....
2663.                   result = xmalloc(len);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=386
Status	New

The function len in git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c at line 2653 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	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	2666	2666
Object	len	len

Code Snippet

File Name	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method	static PSID get_current_user_sid(void)

```
....
2666.                   result = xmalloc(len);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=387
Status	New

The function len in git@@git-v2.42.0-CVE-2021-21300-FP.c at line 2658 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	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	2671	2671
Object	len	len

Code Snippet
File Name git@@git-v2.42.0-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2671.                        result = xmalloc(len);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=388
Status	New

The function len in git@@git-v2.43.1-CVE-2021-21300-FP.c at line 2660 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	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	2673	2673
Object	len	len

Code Snippet
File Name git@@git-v2.43.1-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2673.                        result = xmalloc(len);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=389
Status	New

The function address_size in freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c at line 763 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	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	786	786
Object	address_size	address_size

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	char *stun_determine_ip_address(int family)

```
....
786.     local_ip_address = malloc(address_size + 1);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=390
Status	New

The function address_size in freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c at line 763 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	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	786	786
Object	address_size	address_size

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	char *stun_determine_ip_address(int family)

```
....
786.     local_ip_address = malloc(address_size + 1);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=391
Status	New

The function address_size in freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c at line 763 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	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	786	786
Object	address_size	address_size

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method	char *stun_determine_ip_address(int family)

```
....
786.     local_ip_address = malloc(address_size + 1);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=392
Status	New

The function len in git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c at line 2108 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	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	2120	2120
Object	len	len

Code Snippet

File Name	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method	static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2120.             char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=393
Status	New

The function len in git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c at line 2156 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	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	2168	2168
Object	len	len

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2168.             char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=394
Status	New

The function len in git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c at line 2159 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	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	2171	2171
Object	len	len

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2171.             char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=395
Status	New

The function len in git@@git-v2.30.1-CVE-2021-21300-TP.c at line 2159 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	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	2171	2171
Object	len	len

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2171.           char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=396
Status	New

The function len in git@@git-v2.30.3-CVE-2021-21300-FP.c at line 2164 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	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	2176	2176
Object	len	len

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2176.           char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=397
Status	New

The function len in git@@git-v2.30.3-CVE-2021-21300-FP.c at line 2605 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	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	2615	2615
Object	len	len

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2615.              TOKEN_USER *info = xmalloc((size_t)len);
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=398
Status	New

The function len in git@@git-v2.30.8-CVE-2021-21300-FP.c at line 2164 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	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	2176	2176
Object	len	len

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2176.              char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=399
Status	New

The function len in git@@git-v2.30.8-CVE-2021-21300-FP.c at line 2605 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	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	2615	2615
Object	len	len

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2615.               TOKEN_USER *info = xmalloc((size_t)len);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=400
Status	New

The function len in git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c at line 2163 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	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	2175	2175
Object	len	len

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2175.               char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=401
Status	New

The function len in git@@git-v2.33.0-CVE-2021-21300-FP.c at line 2184 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	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	2196	2196
Object	len	len

Code Snippet
File Name git@@git-v2.33.0-CVE-2021-21300-FP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2196.            char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=402
Status	New

The function len in git@@git-v2.34.1-CVE-2021-21300-FP.c at line 2184 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	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	2196	2196
Object	len	len

Code Snippet
File Name git@@git-v2.34.1-CVE-2021-21300-FP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2196.            char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=403
Status	New

The function len in git@@git-v2.37.0-CVE-2021-21300-FP.c at line 2208 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	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	2220	2220
Object	len	len

Code Snippet

File Name	git@@git-v2.37.0-CVE-2021-21300-FP.c
Method	static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2220.            char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=404
Status	New

The function len in git@@git-v2.37.0-CVE-2021-21300-FP.c at line 2649 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	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	2659	2659
Object	len	len

Code Snippet

File Name	git@@git-v2.37.0-CVE-2021-21300-FP.c
Method	static PSID get_current_user_sid(void)

```
....
2659.            TOKEN_USER *info = xmalloc((size_t)len);
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=405
Status	New

The function len in git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c at line 2206 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	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	2218	2218
Object	len	len

Code Snippet

File Name	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method	static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2218.               char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=406
Status	New

The function len in git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c at line 2647 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	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	2657	2657
Object	len	len

Code Snippet

File Name	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method	static PSID get_current_user_sid(void)

```
....
2657.               TOKEN_USER *info = xmalloc((size_t)len);
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=407
Status	New

The function len in git@@git-v2.39.5-CVE-2021-21300-FP.c at line 2209 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	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	2221	2221
Object	len	len

Code Snippet
File Name git@@git-v2.39.5-CVE-2021-21300-FP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2221.           char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=408
Status	New

The function len in git@@git-v2.39.5-CVE-2021-21300-FP.c at line 2650 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	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	2660	2660
Object	len	len

Code Snippet
File Name git@@git-v2.39.5-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2660.           TOKEN_USER *info = xmalloc((size_t)len);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=409
Status	New

The function len in git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c at line 2212 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	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	2224	2224
Object	len	len

Code Snippet

File Name	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method	static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2224.               char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=410
Status	New

The function len in git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c at line 2653 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	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	2663	2663
Object	len	len

Code Snippet

File Name	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method	static PSID get_current_user_sid(void)

```
....
2663.               TOKEN_USER *info = xmalloc((size_t)len);
```

Wrong Size t Allocation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=411
Status	New

The function len in git@@git-v2.42.0-CVE-2021-21300-FP.c at line 2217 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	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	2229	2229
Object	len	len

Code Snippet
File Name git@@git-v2.42.0-CVE-2021-21300-FP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2229.             char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=412
Status	New

The function len in git@@git-v2.42.0-CVE-2021-21300-FP.c at line 2658 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	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	2668	2668
Object	len	len

Code Snippet
File Name git@@git-v2.42.0-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2668.             TOKEN_USER *info = xmalloc((size_t)len);
```

Wrong Size t Allocation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=413
Status	New

The function len in git@@git-v2.43.1-CVE-2021-21300-FP.c at line 2219 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	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	2231	2231
Object	len	len

Code Snippet
File Name git@@git-v2.43.1-CVE-2021-21300-FP.c
Method static char *get_extended_user_info(enum EXTENDED_NAME_FORMAT type)

```
....
2231.           char *converted = xmalloc((len *= 3));
```

Wrong Size t Allocation\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=414
Status	New

The function len in git@@git-v2.43.1-CVE-2021-21300-FP.c at line 2660 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	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	2670	2670
Object	len	len

Code Snippet
File Name git@@git-v2.43.1-CVE-2021-21300-FP.c
Method static PSID get_current_user_sid(void)

```
....
2670.           TOKEN_USER *info = xmalloc((size_t)len);
```

Heap Inspection

Query Path:
CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Heap Inspection\Path 1:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1997
Status	New

Method keyring_get at line 166 of git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Line	170	170
Object	password_data	password_data

Code Snippet

File Name	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Method	static int keyring_get(struct credential *c)

```
....
170.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1998
Status	New

Method keyring_erase at line 258 of git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet

File Name	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Method	static int keyring_erase(struct credential *c)

```
....
262.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1999
Status	New

Method keyring_get at line 166 of git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Line	170	170
Object	password_data	password_data

Code Snippet

File Name	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Method	static int keyring_get(struct credential *c)

```
....
170.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2000
Status	New

Method keyring_erase at line 258 of git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet

File Name	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Method	static int keyring_erase(struct credential *c)

```
....
262.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 5:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2001
Status	New

Method keyring_get at line 166 of git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Line	170	170
Object	password_data	password_data

Code Snippet

File Name	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method	static int keyring_get(struct credential *c)

```
....
170.        GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2002
Status	New

Method keyring_erase at line 258 of git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet

File Name	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method	static int keyring_erase(struct credential *c)

```
....
262.        GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=2003
Status	New

Method keyring_get at line 166 of git@@git-v2.30.1-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.30.1-CVE-2020-5260-FP.c	git@@git-v2.30.1-CVE-2020-5260-FP.c
Line	170	170
Object	password_data	password_data

Code Snippet
File Name git@@git-v2.30.1-CVE-2020-5260-FP.c
Method static int keyring_get(struct credential *c)

```
....
170.        GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2004
Status	New

Method keyring_erase at line 258 of git@@git-v2.30.1-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.30.1-CVE-2020-5260-FP.c	git@@git-v2.30.1-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet
File Name git@@git-v2.30.1-CVE-2020-5260-FP.c
Method static int keyring_erase(struct credential *c)

```
....
262.        GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2005
Status	New

Method keyring_get at line 166 of git@@git-v2.30.3-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.30.3-CVE-2020-5260-FP.c	git@@git-v2.30.3-CVE-2020-5260-FP.c
Line	170	170
Object	password_data	password_data

Code Snippet
File Name git@@git-v2.30.3-CVE-2020-5260-FP.c
Method static int keyring_get(struct credential *c)

```
....
170.        GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2006
Status	New

Method keyring_erase at line 258 of git@@git-v2.30.3-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.30.3-CVE-2020-5260-FP.c	git@@git-v2.30.3-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet
File Name git@@git-v2.30.3-CVE-2020-5260-FP.c
Method static int keyring_erase(struct credential *c)

```
....
262.        GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2007
Status	New

Method keyring_get at line 166 of git@@git-v2.30.8-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.30.8-CVE-2020-5260-FP.c	git@@git-v2.30.8-CVE-2020-5260-FP.c
Line	170	170
Object	password_data	password_data

Code Snippet
File Name git@@git-v2.30.8-CVE-2020-5260-FP.c
Method static int keyring_get(struct credential *c)

```
....
170.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2008
Status	New

Method keyring_erase at line 258 of git@@git-v2.30.8-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.30.8-CVE-2020-5260-FP.c	git@@git-v2.30.8-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet
File Name git@@git-v2.30.8-CVE-2020-5260-FP.c
Method static int keyring_erase(struct credential *c)

```
....
262.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2009
Status	New

Method keyring_get at line 166 of git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination

File	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Line	170	170
Object	password_data	password_data

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Method static int keyring_get(struct credential *c)

```
....
170.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2010
Status	New

Method keyring_erase at line 258 of git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Method static int keyring_erase(struct credential *c)

```
....
262.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2011
Status	New

Method keyring_get at line 166 of git@@git-v2.33.0-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination

File	git@@git-v2.33.0-CVE-2020-5260-FP.c	git@@git-v2.33.0-CVE-2020-5260-FP.c
Line	170	170
Object	password_data	password_data

Code Snippet
File Name	git@@git-v2.33.0-CVE-2020-5260-FP.c
Method	static int keyring_get(struct credential *c)

```
....
170.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2012
Status	New

Method keyring_erase at line 258 of git@@git-v2.33.0-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.33.0-CVE-2020-5260-FP.c	git@@git-v2.33.0-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet
File Name	git@@git-v2.33.0-CVE-2020-5260-FP.c
Method	static int keyring_erase(struct credential *c)

```
....
262.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2013
Status	New

Method keyring_get at line 166 of git@@git-v2.34.1-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.34.1-CVE-2020-5260-FP.c	git@@git-v2.34.1-CVE-2020-5260-FP.c

Line	170	170
Object	password_data	password_data

Code Snippet
File Name git@@git-v2.34.1-CVE-2020-5260-FP.c
Method static int keyring_get(struct credential *c)

```
....
170.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2014
Status	New

Method keyring_erase at line 258 of git@@git-v2.34.1-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.34.1-CVE-2020-5260-FP.c	git@@git-v2.34.1-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet
File Name git@@git-v2.34.1-CVE-2020-5260-FP.c
Method static int keyring_erase(struct credential *c)

```
....
262.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2015
Status	New

Method keyring_get at line 166 of git@@git-v2.37.0-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.37.0-CVE-2020-5260-FP.c	git@@git-v2.37.0-CVE-2020-5260-FP.c
Line	170	170

Object	password_data	password_data

Code Snippet
File Name	git@@git-v2.37.0-CVE-2020-5260-FP.c
Method	static int keyring_get(struct credential *c)

```
....
170.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2016
Status	New

Method keyring_erase at line 258 of git@@git-v2.37.0-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.37.0-CVE-2020-5260-FP.c	git@@git-v2.37.0-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet
File Name	git@@git-v2.37.0-CVE-2020-5260-FP.c
Method	static int keyring_erase(struct credential *c)

```
....
262.         GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2017
Status	New

Method keyring_get at line 166 of git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Line	170	170
Object	password_data	password_data

Code Snippet

File Name	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Method	static int keyring_get(struct credential *c)

```
....
170.        GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2018
Status	New

Method keyring_erase at line 258 of git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet

File Name	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Method	static int keyring_erase(struct credential *c)

```
....
262.        GnomeKeyringNetworkPasswordData *password_data;
```

Heap Inspection\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2019
Status	New

Method keyring_get at line 166 of git@@git-v2.39.5-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.39.5-CVE-2020-5260-FP.c	git@@git-v2.39.5-CVE-2020-5260-FP.c
Line	170	170
Object	password_data	password_data

Code Snippet

File Name	git@@git-v2.39.5-CVE-2020-5260-FP.c
Method	static int keyring_get(struct credential *c)

```
....
170.        GnomeKeyringNetworkPasswordData *password_data;
```

Heavy Inspection\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2020
Status	New

Method keyring_erase at line 258 of git@@git-v2.39.5-CVE-2020-5260-FP.c defines password_data, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password_data, this variable is never cleared from memory.

	Source	Destination
File	git@@git-v2.39.5-CVE-2020-5260-FP.c	git@@git-v2.39.5-CVE-2020-5260-FP.c
Line	262	262
Object	password_data	password_data

Code Snippet

File Name	git@@git-v2.39.5-CVE-2020-5260-FP.c
Method	static int keyring_erase(struct credential *c)

```
....
262.        GnomeKeyringNetworkPasswordData *password_data;
```

Inadequate Encryption Strength

Query Path:
CPP\Cx\CPP Medium Threat\Inadequate Encryption Strength Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: SC-13 Cryptographic Protection (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Inadequate Encryption Strength\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2315
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 94 of FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c at line 94.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	116	130
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_make_md5_digest(struct eigrp_interface *ei, struct stream *s,

```
....
116.         keychain = keychain_lookup(ei->params.auth_keychain);
....
130.               MD5Update(&ctx, key->string, strlen(key->string));
```

Inadequate Encryption Strength\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2316
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 94 of FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c at line 94.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	116	132
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_make_md5_digest(struct eigrp_interface *ei, struct stream *s,

```
....
116.         keychain = keychain_lookup(ei->params.auth_keychain);
....
132.                     MD5Update(&ctx, zeropad, 16 - strlen(key-
>string));
```

Inadequate Encryption Strength\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2317
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 94 of FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c at line 94.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	116	137
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_make_md5_digest(struct eigrp_interface *ei, struct stream *s,

```
....
116.        keychain = keychain_lookup(ei->params.auth_keychain);
....
137.                MD5Update(&ctx, key->string, strlen(key->string));
```

Inadequate Encryption Strength\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2318
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 94 of FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c at line 94.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	116	139
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_make_md5_digest(struct eigrp_interface *ei, struct stream *s,

```
....
116.        keychain = keychain_lookup(ei->params.auth_keychain);
....
139.                        MD5Update(&ctx, zeropad, 16 - strlen(key-
>string));
```

Inadequate Encryption Strength\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=2319
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 163 of FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c at line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	197	214
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
197.        keychain = keychain_lookup(nbr->ei->params.auth_keychain);
....
214.              MD5Update(&ctx, key->string, strlen(key->string));
```

Inadequate Encryption Strength\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2320
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 163 of FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c at line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	197	216
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
197.        keychain = keychain_lookup(nbr->ei->params.auth_keychain);
....
216.                    MD5Update(&ctx, zeropad, 16 - strlen(key-
>string));
```

Inadequate Encryption Strength\Path 7:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2321
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 163 of FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c at line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	197	221
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
197.        keychain = keychain_lookup(nbr->ei->params.auth_keychain);
....
221.              MD5Update(&ctx, key->string, strlen(key->string));
```

Inadequate Encryption Strength\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2322
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 163 of FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c at line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	197	223
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
197.        keychain = keychain_lookup(nbr->ei->params.auth_keychain);
....
223.                    MD5Update(&ctx, zeropad, 16 - strlen(key->string));
```

Inadequate Encryption Strength\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2323
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 94 of FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c at line 94.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	116	130
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method int eigrp_make_md5_digest(struct eigrp_interface *ei, struct stream *s,

```
....
116.        keychain = keychain_lookup(ei->params.auth_keychain);
....
130.              MD5Update(&ctx, key->string, strlen(key->string));
```

Inadequate Encryption Strength\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2324
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 94 of FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c at line 94.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	116	132
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method int eigrp_make_md5_digest(struct eigrp_interface *ei, struct stream *s,

```
....
116.        keychain = keychain_lookup(ei->params.auth_keychain);
....
132.                    MD5Update(&ctx, zeropad, 16 - strlen(key-
>string));
```

Inadequate Encryption Strength\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2325
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 94 of FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c at line 94.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	116	137
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method int eigrp_make_md5_digest(struct eigrp_interface *ei, struct stream *s,

```
....
116.        keychain = keychain_lookup(ei->params.auth_keychain);
....
137.              MD5Update(&ctx, key->string, strlen(key->string));
```

Inadequate Encryption Strength\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2326
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 94 of FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c at line 94.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	116	139
Object	auth_keychain	MD5Update

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method	int eigrp_make_md5_digest(struct eigrp_interface *ei, struct stream *s,

```
....
116.        keychain = keychain_lookup(ei->params.auth_keychain);
....
139.                    MD5Update(&ctx, zeropad, 16 - strlen(key-
>string));
```

Inadequate Encryption Strength\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2327
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 163 of FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c at line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	197	214
Object	auth_keychain	MD5Update

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method	int eigrp_check_md5_digest(struct stream *s,

```
....
197.        keychain = keychain_lookup(nbr->ei->params.auth_keychain);
....
214.                MD5Update(&ctx, key->string, strlen(key->string));
```

Inadequate Encryption Strength\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2328
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 163 of FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c at line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c

Line	197	216
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
197.        keychain = keychain_lookup(nbr->ei->params.auth_keychain);
....
216.                    MD5Update(&ctx, zeropad, 16 - strlen(key-
>string));
```

Inadequate Encryption Strength\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2329
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 163 of FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c at line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	197	221
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
197.        keychain = keychain_lookup(nbr->ei->params.auth_keychain);
....
221.              MD5Update(&ctx, key->string, strlen(key->string));
```

Inadequate Encryption Strength\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2330
Status	New

The application uses a weak cryptographic algorithm, MD5Update at line 163 of FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c, to protect sensitive personal information auth_keychain, from FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c at line 163.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	197	223
Object	auth_keychain	MD5Update

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method int eigrp_check_md5_digest(struct stream *s,

```
....
197.        keychain = keychain_lookup(nbr->ei->params.auth_keychain);
....
223.                    MD5Update(&ctx, zeropad, 16 - strlen(key-
>string));
```

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=1000020&projectid=15&pathid=2583
Status	New

The application protects passwords with HMAC in stun_encode_message_integrity, of freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c at line 434, using a cryptographic hash padded_text. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	455	455
Object	padded_text	HMAC

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
455.       sha1_hmac = HMAC(EVP_sha1(), pwd->data, pwd->size,
padded_text, padded_len, NULL, &dig_len);
```

Use of a One Way Hash without a Salt\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2584
Status	New

The application protects passwords with HMAC in stun_encode_message_integrity, of freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c at line 434, using a cryptographic hash 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	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	733	455
Object	buf	HMAC

Code Snippet

File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c

Method int stun_encode_message(stun_msg_t *msg, stun_buffer_t *pwd) {

```
....
733.         memcpy(buf+len, (void *)attr->enc_buf.data, attr-
>enc_buf.size);
```

File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c

Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
455.       sha1_hmac = HMAC(EVP_sha1(), pwd->data, pwd->size,
padded_text, padded_len, NULL, &dig_len);
```

Use of a One Way Hash without a Salt\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2585
Status	New

The application protects passwords with HMAC in stun_encode_message_integrity, of freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c at line 434, using a cryptographic hash 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	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	458	458
Object	buf	HMAC

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
458.        sha1_hmac = HMAC(EVP_sha1(), pwd->data, pwd->size, buf, len,
NULL, &dig_len);
```

Use of a One Way Hash without a Salt\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2586
Status	New

The application protects passwords with HMAC in stun_validate_message_integrity, of freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c at line 499, using a cryptographic hash padded_text. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	531	531
Object	padded_text	HMAC

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method int stun_validate_message_integrity(stun_msg_t *msg, stun_buffer_t *pwd)

```
....
531.    memcpy(dig, HMAC(EVP_sha1(), pwd->data, pwd->size, padded_text,
padded_len, NULL, &dig_len), 20);
```

Use of a One Way Hash without a Salt\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2587
Status	New

The application protects passwords with HMAC in stun_encode_message_integrity, of freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c at line 434, using a cryptographic hash padded_text. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	455	455
Object	padded_text	HMAC

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
455.       sha1_hmac = HMAC(EVP_sha1(), pwd->data, pwd->size,
padded_text, padded_len, NULL, &dig_len);
```

Use of a One Way Hash without a Salt\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2588
Status	New

The application protects passwords with HMAC in stun_encode_message_integrity, of freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c at line 434, using a cryptographic hash 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	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	733	455
Object	buf	HMAC

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_message(stun_msg_t *msg, stun_buffer_t *pwd) {

```
....
733.         memcpy(buf+len, (void *)attr->enc_buf.data, attr-
>enc_buf.size);
```

File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
455.        sha1_hmac = HMAC(EVP_sha1(), pwd->data, pwd->size,
padded_text, padded_len, NULL, &dig_len);
```

Use of a One Way Hash without a Salt\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2589
Status	New

The application protects passwords with HMAC in stun_encode_message_integrity, of freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c at line 434, using a cryptographic hash 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	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	458	458
Object	buf	HMAC

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
458.        sha1_hmac = HMAC(EVP_sha1(), pwd->data, pwd->size, buf, len,
NULL, &dig_len);
```

Use of a One Way Hash without a Salt\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2590
Status	New

The application protects passwords with HMAC in stun_validate_message_integrity, of freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c at line 499, using a cryptographic hash padded_text. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	531	531
Object	padded_text	HMAC

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method	int stun_validate_message_integrity(stun_msg_t *msg, stun_buffer_t *pwd)

```
....
531.    memcpy(dig, HMAC(EVP_sha1(), pwd->data, pwd->size, padded_text,
padded_len, NULL, &dig_len), 20);
```

Use of a One Way Hash without a Salt\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2591
Status	New

The application protects passwords with HMAC in stun_encode_message_integrity, of freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c at line 434, using a cryptographic hash padded_text. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	455	455
Object	padded_text	HMAC

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method	int stun_encode_message_integrity(stun_attr_t *attr,

```
....
455.      sha1_hmac = HMAC(EVP_sha1(), pwd->data, pwd->size,
padded_text, padded_len, NULL, &dig_len);
```

Use of a One Way Hash without a Salt\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2592
Status	New

The application protects passwords with HMAC in stun_encode_message_integrity, of freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c at line 434, using a cryptographic hash 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	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	733	455

Object	buf	HMAC

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method int stun_encode_message(stun_msg_t *msg, stun_buffer_t *pwd) {

```
....
733.        memcpy(buf+len, (void *)attr->enc_buf.data, attr-
>enc_buf.size);
```

File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
455.        sha1_hmac = HMAC(EVP_sha1(), pwd->data, pwd->size,
padded_text, padded_len, NULL, &dig_len);
```

Use of a One Way Hash without a Salt\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2593
Status	New

The application protects passwords with HMAC in stun_encode_message_integrity, of freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c at line 434, using a cryptographic hash 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	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	458	458
Object	buf	HMAC

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method int stun_encode_message_integrity(stun_attr_t *attr,

```
....
458.        sha1_hmac = HMAC(EVP_sha1(), pwd->data, pwd->size, buf, len,
NULL, &dig_len);
```

Use of a One Way Hash without a Salt\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2594

Status	New

The application protects passwords with HMAC in stun_validate_message_integrity, of freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c at line 499, using a cryptographic hash padded_text. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	531	531
Object	padded_text	HMAC

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method int stun_validate_message_integrity(stun_msg_t *msg, stun_buffer_t *pwd)

```
....
531.    memcpy(dig, HMAC(EVP_sha1(), pwd->data, pwd->size, padded_text,
padded_len, NULL, &dig_len), 20);
```

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=1000020&projectid=15&pathid=415
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1290 of FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c
Line	1367	1367
Object	AssignExpr	AssignExpr

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c
Method static void bgp_peer_send_gr_capability(struct stream *s, struct peer *peer,

```
....
1367.        len = stream_get_endp(s) - capp - 1;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=416
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1290 of FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c
Line	1363	1363
Object	AssignExpr	AssignExpr

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-31489-FP.c
Method static void bgp_peer_send_gr_capability(struct stream *s, struct peer *peer,

```
....
1363.        len = stream_get_endp(s) - rcapp - 1;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=417
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1327 of FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c
Line	1404	1404
Object	AssignExpr	AssignExpr

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c
Method static void bgp_peer_send_gr_capability(struct stream *s, struct peer *peer,

```
....
1404.        len = stream_get_endp(s) - capp - 1;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=418
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1327 of FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c
Line	1400	1400
Object	AssignExpr	AssignExpr

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2023-31489-FP.c
Method	static void bgp_peer_send_gr_capability(struct stream *s, struct peer *peer,

```
....
1400.        len = stream_get_endp(s) - rcapp - 1;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=419
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1327 of FRRouting@@frr-frr-8.0.1-CVE-2023-41361-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-41361-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-41361-TP.c
Line	1404	1404
Object	AssignExpr	AssignExpr

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2023-41361-TP.c
Method	static void bgp_peer_send_gr_capability(struct stream *s, struct peer *peer,

```
....
1404.        len = stream_get_endp(s) - capp - 1;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=420
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1327 of FRRouting@@frr-frr-8.0.1-CVE-2023-41361-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-41361-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-41361-TP.c
Line	1400	1400
Object	AssignExpr	AssignExpr

Code Snippet

File Name	FRRouting@@frr-frr-8.0.1-CVE-2023-41361-TP.c
Method	static void bgp_peer_send_gr_capability(struct stream *s, struct peer *peer,

```
....
1400.        len = stream_get_endp(s) - rcapp - 1;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=421
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1509 of FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c
Line	1594	1594
Object	AssignExpr	AssignExpr

Code Snippet

File Name	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c
Method	static void bgp_peer_send_gr_capability(struct stream *s, struct peer *peer,

```
....
1594.        len = stream_get_endp(s) - capp - 1;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=422
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1509 of FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c
Line	1590	1590
Object	AssignExpr	AssignExpr

Code Snippet

File Name	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c
Method	static void bgp_peer_send_gr_capability(struct stream *s, struct peer *peer,

```
....
1590.        len = stream_get_endp(s) - rcapp - 1;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=423
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1599 of FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c
Line	1643	1643
Object	AssignExpr	AssignExpr

Code Snippet

File Name	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c
Method	static void bgp_peer_send_llgr_capability(struct stream *s, struct peer *peer,

```
....
1643.        len = stream_get_endp(s) - capp - 1;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=424
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1599 of FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c
Line	1639	1639
Object	AssignExpr	AssignExpr

Code Snippet

File Name	FRRouting@@frr-frr-8.4.4-CVE-2023-31489-FP.c
Method	static void bgp_peer_send_llgr_capability(struct stream *s, struct peer *peer,

```
....
1639.        len = stream_get_endp(s) - rcapp - 1;
```

Use of Uninitialized Variable

Query Path:

CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Variable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2021
Status	New

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	2728	2739
Object	is_member	is_member

Code Snippet
File Name git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method int is_path_owned_by_current_sid(const char *path, struct strbuf *report)

```
....
2728.                   BOOL is_member;
....
2739.                           is_member)
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2022
Status	New

	Source	Destination
File	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	2731	2742
Object	is_member	is_member

Code Snippet
File Name git@@git-v2.39.5-CVE-2021-21300-FP.c
Method int is_path_owned_by_current_sid(const char *path, struct strbuf *report)

```
....
2731.                   BOOL is_member;
....
2742.                           is_member)
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2023
Status	New

	Source	Destination
File	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	2734	2745
Object	is_member	is_member

Code Snippet
File Name git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method int is_path_owned_by_current_sid(const char *path, struct strbuf *report)

```
....
2734.                   BOOL is_member;
....
2745.                          is_member)
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2024
Status	New

	Source	Destination
File	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	2739	2750
Object	is_member	is_member

Code Snippet

File Name	git@@git-v2.42.0-CVE-2021-21300-FP.c
Method	int is_path_owned_by_current_sid(const char *path, struct strbuf *report)

```
....
2739.                   BOOL is_member;
....
2750.                          is_member)
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2025
Status	New

	Source	Destination
File	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	2741	2752
Object	is_member	is_member

Code Snippet

File Name	git@@git-v2.43.1-CVE-2021-21300-FP.c
Method	int is_path_owned_by_current_sid(const char *path, struct strbuf *report)

```
....
2741.                   BOOL is_member;
....
2752.                          is_member)
```

Use of Hard coded Cryptographic Key

Query Path:
CPP\Cx\CPP Medium Threat\Use of Hard coded Cryptographic Key Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Hard coded Cryptographic Key\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1993
Status	New

The variable key_sequence at line 1238 of FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	1251	1251
Object	key_sequence	key_sequence

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method uint16_t eigrp_add_authTLV_MD5_to_stream(struct stream *s,

```
....
1251.        authTLV->key_sequence = 0;
```

Use of Hard coded Cryptographic Key\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1994
Status	New

The variable key_sequence at line 1278 of FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Line	1291	1291
Object	key_sequence	key_sequence

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2023-46752-TP.c
Method	uint16_t eigrp_add_authTLV_SHA256_to_stream(struct stream *s,

```
....
1291.       authTLV->key_sequence = 0;
```

Use of Hard coded Cryptographic Key\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1995
Status	New

The variable key_sequence at line 1238 of FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	1251	1251
Object	key_sequence	key_sequence

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method	uint16_t eigrp_add_authTLV_MD5_to_stream(struct stream *s,

```
....
1251.       authTLV->key_sequence = 0;
```

Use of Hard coded Cryptographic Key\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1996
Status	New

The variable key_sequence at line 1278 of FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Line	1291	1291
Object	key_sequence	key_sequence

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-46752-TP.c
Method	uint16_t eigrp_add_authTLV_SHA256_to_stream(struct stream *s,

```
....
1291.        authTLV->key_sequence = 0;
```

Off by One Error in Methods

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Methods Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Off by One Error in Methods\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=380
Status	New

The buffer allocated by sizeof in FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c at line 749 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	751	751
Object	what_stop	sizeof

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static void set_what_stop(const char *str)

```
....
751.        strncpy(what_stop, str, sizeof(what_stop));
```

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=1000020&projectid=15&pathid=2924
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by doblend at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2777.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	2811
Object	null	doblend

Code Snippet
File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method TT_Get_MM_Blend(TT_Face face,

```
....
2811.       if ( face->doblend )
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2925
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by face at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 1185.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	1204
Object	null	face

Code Snippet
File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method ft_var_load_mvar(TT_Face face)

```
....
1204.       error = face->goto_table( face, TTAG_MVAR, stream, &table_len
);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2926
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by is_cff2 at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2505.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	2565
Object	null	is_cff2

Code Snippet

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method tt_set_mm_blend(TT_Face face,

```
....
2565.       if ( !face->is_cff2 && !blend->glyphoffsets )
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2927

Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by face at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 333.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	351
Object	null	face

Code Snippet
File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

▼

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method ft_var_load_avar(TT_Face face)

```
....
351.      error = face->goto_table( face, TTAG_avar, stream, &table_len
);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2928
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by blend at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2505.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	2530
Object	null	blend

Code Snippet
File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method tt_set_mm_blend(TT_Face face,

```
....
2530.       if ( !face->blend )
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2929
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by blend at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2858.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	2952
Object	null	blend

Code Snippet

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method TT_Set_Var_Design(TT_Face face,

```
....
2952.       if ( !face->blend->avar_loaded )
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2930
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by doblend at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3000.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	2045	3034
Object	null	doblend

Code Snippet

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method TT_Get_Var_Design(TT_Face face,

```
....
3034.       if ( face->doblend )
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2931
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3752 is not initialized when it is used by x at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3526.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	3763	3544
Object	null	x

Code Snippet

File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3763.       FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

▼

File Name	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method	tt_delta_shift(int p1,

```
....
3544.        out_points[p].x += delta.x;
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2932
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3752 is not initialized when it is used by x at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3526.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	3763	3550
Object	null	x

Code Snippet

File Name	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method	TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3763.      FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

▼

File Name	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method	tt_delta_shift(int p1,

```
....
3550.        out_points[p].x += delta.x;
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2933
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3752 is not initialized when it is used by y at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3526.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	3763	3551
Object	null	y

Code Snippet
File Name   freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method   TT_Vary_Apply_Glyph_Deltas(TT_Face   face,

```
....
3763.       FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name   freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method   tt_delta_shift(int   p1,

```
....
3551.          out_points[p].y += delta.y;
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2934
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3752 is not initialized when it is used by y at freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c in line 3526.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	3763	3545
Object	null	y

Code Snippet
File Name   freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method   TT_Vary_Apply_Glyph_Deltas(TT_Face   face,

```
....
3763.       FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name   freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3545.         out_points[p].y += delta.y;
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2935
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by doblend at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2777.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	2045	2811
Object	null	doblend

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method TT_Get_MM_Blend(TT_Face face,

```
....
2811.       if ( face->doblend )
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2936
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by face at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 1185.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-	freetype@@freetype-VER-2-10-3-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	2045	1204
Object	null	face

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

▼

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method ft_var_load_mvar(TT_Face face)

```
....
1204.       error = face->goto_table( face, TTAG_MVAR, stream, &table_len
);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2937
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by is_cff2 at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2505.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	2045	2565
Object	null	is_cff2

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

▼

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method tt_set_mm_blend(TT_Face face,

```
....
2565.       if ( !face->is_cff2 && !blend->glyphoffsets )
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2938
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by face at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 333.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	2045	351
Object	null	face

Code Snippet

File Name	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*              mmvar = NULL;
```

File Name	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method	ft_var_load_avar(TT_Face face)

```
....
351.      error = face->goto_table( face, TTAG_avar, stream, &table_len
);
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2939
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by blend at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2505.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-	freetype@@freetype-VER-2-10-3-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	2045	2530
Object	null	blend

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method tt_set_mm_blend(TT_Face face,

```
....
2530.       if ( !face->blend )
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2940
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by blend at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2858.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	2045	2952
Object	null	blend

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method TT_Set_Var_Design(TT_Face face,

```
....
2952.       if ( !face->blend->avar_loaded )
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2941
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 2036 is not initialized when it is used by doblend at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3000.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	2045	3034
Object	null	doblend

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2045.       FT_MM_Var*           mmvar = NULL;
```

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method TT_Get_Var_Design(TT_Face face,

```
....
3034.       if ( face->doblend )
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2942
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3752 is not initialized when it is used by y at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3526.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Line	3763	3551
Object	null	y

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3763.       FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3551.         out_points[p].y += delta.y;
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2943
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3752 is not initialized when it is used by x at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3526.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	3763	3550
Object	null	x

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3763.       FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3550.         out_points[p].x += delta.x;
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2944
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3752 is not initialized when it is used by y at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3526.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	3763	3545
Object	null	y

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3763.       FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3545.         out_points[p].y += delta.y;
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2945
Status	New

The variable declared in null at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3752 is not initialized when it is used by x at freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c in line 3526.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-	freetype@@freetype-VER-2-10-3-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	3763	3544
Object	null	x

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3763.      FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3544.         out_points[p].x += delta.x;
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2946
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by doblend at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2789.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	2056	2823
Object	null	doblend

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2056.      FT_MM_Var*          mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c

Method TT_Get_MM_Blend(TT_Face face,

```
....
2823.       if ( face->doblend )
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2947
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by face at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 1195.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	2056	1214
Object	null	face

Code Snippet

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2056.       FT_MM_Var*             mmvar = NULL;
```

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	ft_var_load_mvar(TT_Face face)

```
....
1214.       error = face->goto_table( face, TTAG_MVAR, stream, &table_len
);
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2948
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by is_cff2 at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2516.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-	freetype@@freetype-VER-2-11-0-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	2056	2576
Object	null	is_cff2

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2056.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c

Method tt_set_mm_blend(TT_Face face,

```
....
2576.       if ( !face->is_cff2 && !blend->glyphoffsets )
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2949
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by face at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 333.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	2056	351
Object	null	face

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2056.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c

Method ft_var_load_avar(TT_Face face)

```
....
351.        error = face->goto_table( face, TTAG_avar, stream, &table_len
);
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2950
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by blend at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2516.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	2056	2541
Object	null	blend

Code Snippet

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2056.       FT_MM_Var*            mmvar = NULL;
```

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	tt_set_mm_blend(TT_Face face,

```
....
2541.       if ( !face->blend )
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2951
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by blend at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2870.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-	freetype@@freetype-VER-2-11-0-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	2056	2964
Object	null	blend

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2056.       FT_MM_Var*             mmvar = NULL;
```

▼

File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c

Method TT_Set_Var_Design(TT_Face face,

```
....
2964.       if ( !face->blend->avar_loaded )
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2952
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 2047 is not initialized when it is used by doblend at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3012.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	2056	3046
Object	null	doblend

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2056.       FT_MM_Var*             mmvar = NULL;
```

▼

File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c

Method TT_Get_Var_Design(TT_Face face,

```
....
3046.       if ( face->doblend )
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2953
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3764 is not initialized when it is used by y at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3538.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	3775	3563
Object	null	y

Code Snippet

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3775.       FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method	tt_delta_shift(int p1,

```
....
3563.         out_points[p].y += delta.y;
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2954
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3764 is not initialized when it is used by x at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3538.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-	freetype@@freetype-VER-2-11-0-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	3775	3562
Object	null	x

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3775.      FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3562.         out_points[p].x += delta.x;
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2955
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3764 is not initialized when it is used by y at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3538.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	3775	3557
Object	null	y

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3775.      FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3557.         out_points[p].y += delta.y;
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2956
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3764 is not initialized when it is used by x at freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c in line 3538.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	3775	3556
Object	null	x

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3775.       FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3556.         out_points[p].x += delta.x;
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2957
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by face at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 358.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-	freetype@@freetype-VER-2-11-1-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	2125	376
Object	null	face

Code Snippet

File Name	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*            mmvar = NULL;
```

▼

File Name	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method	ft_var_load_avar(TT_Face face)

```
....
376.       error = face->goto_table( face, TTAG_avar, stream, &table_len
);
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2958
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by blend at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2939.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	2125	3033
Object	null	blend

Code Snippet

File Name	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method	TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*            mmvar = NULL;
```

▼

File Name	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method	TT_Set_Var_Design(TT_Face face,

```
....
3033.       if ( !face->blend->avar_loaded )
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2959
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by doblend at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2858.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	2125	2892
Object	null	doblend

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method TT_Get_MM_Blend(TT_Face face,

```
....
2892.       if ( face->doblend )
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2960
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by face at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 1267.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Line	2125	1286
Object	null	face

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method ft_var_load_mvar(TT_Face face)

```
....
1286.       error = face->goto_table( face, TTAG_MVAR, stream, &table_len
);
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2961
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by is_cff2 at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2585.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	2125	2645
Object	null	is_cff2

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method tt_set_mm_blend(TT_Face face,

```
....
2645.        if ( !face->is_cff2 && !blend->glyphoffsets )
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2962
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by blend at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2585.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	2125	2610
Object	null	blend

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2125.        FT_MM_Var*          mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method tt_set_mm_blend(TT_Face face,

```
....
2610.        if ( !face->blend )
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2963
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 2116 is not initialized when it is used by doblend at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3081.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Line	2125	3115
Object	null	doblend

Code Snippet

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method TT_Get_MM_Var(TT_Face face,

```
....
2125.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method TT_Get_Var_Design(TT_Face face,

```
....
3115.       if ( face->doblend )
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2964
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3848 is not initialized when it is used by y at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3622.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	3859	3641
Object	null	y

Code Snippet

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3859.       FT_Vector*  points_out = NULL;   /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3641.         out_points[p].y += delta.y;
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2965
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3848 is not initialized when it is used by x at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3622.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	3859	3640
Object	null	x

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3859.       FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3640.         out_points[p].x += delta.x;
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2966
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3848 is not initialized when it is used by y at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3622.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-	freetype@@freetype-VER-2-11-1-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	3859	3647
Object	null	y

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3859.      FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3647.        out_points[p].y += delta.y;
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2967
Status	New

The variable declared in null at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3848 is not initialized when it is used by x at freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c in line 3622.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	3859	3646
Object	null	x

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method TT_Vary_Apply_Glyph_Deltas(TT_Face face,

```
....
3859.      FT_Vector*  points_out = NULL;  /* coordinates in 16.16
format */
```

File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c

Method tt_delta_shift(int p1,

```
....
3646.        out_points[p].x += delta.x;
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2968
Status	New

The variable declared in null at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by face at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 354.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	2118	370
Object	null	face

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2118.      FT_MM_Var*          mmvar = NULL;
```

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method ft_var_load_avar(TT_Face face)

```
....
370.     error = face->goto_table( face, TTAG_avar, stream, &table_len
);
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2969
Status	New

The variable declared in null at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by blend at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2930.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-	freetype@@freetype-VER-2-12-0-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	2118	3024
Object	null	blend

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2118.       FT_MM_Var*            mmvar = NULL;
```

▼

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method TT_Set_Var_Design(TT_Face face,

```
....
3024.       if ( !face->blend->avar_loaded )
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2970
Status	New

The variable declared in null at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by doblend at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2849.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	2118	2883
Object	null	doblend

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2118.       FT_MM_Var*            mmvar = NULL;
```

▼

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method TT_Get_MM_Blend(TT_Face face,

```
....
2883.       if ( face->doblend )
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2971
Status	New

The variable declared in null at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by face at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 1260.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	2118	1279
Object	null	face

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2118.       FT_MM_Var*            mmvar = NULL;
```

▼

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method ft_var_load_mvar(TT_Face face)

```
....
1279.       error = face->goto_table( face, TTAG_MVAR, stream, &table_len
);
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2972
Status	New

The variable declared in null at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by is_cff2 at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2578.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-	freetype@@freetype-VER-2-12-0-CVE-

	2023-2004-TP.c	2023-2004-TP.c
Line	2118	2638
Object	null	is_cff2

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2118.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method tt_set_mm_blend(TT_Face face,

```
....
2638.       if ( !face->is_cff2 && !blend->glyphoffsets )
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2973
Status	New

The variable declared in null at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2109 is not initialized when it is used by blend at freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c in line 2578.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	2118	2603
Object	null	blend

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method TT_Get_MM_Var(TT_Face face,

```
....
2118.       FT_MM_Var*            mmvar = NULL;
```

File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c

Method tt_set_mm_blend(TT_Face face,

```
....
2603.       if ( !face->blend )
```

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=1000020&projectid=15&pathid=2331
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet

File Name	git@@git-v2.26.0-rc1-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2332
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	158	158
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static int read_yes_no_answer(void)

```
....
158.         if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2333
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2334
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	158	158
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method static int read_yes_no_answer(void)

```
....
158.         if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2335
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2336
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	158	158
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method static int read_yes_no_answer(void)

```
....
158.        if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2337

Status New

	Source	Destination
File	git@@git-v2.30.1-CVE-2020-5260-FP.c	git@@git-v2.30.1-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.30.1-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2338
Status New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	158	158
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method static int read_yes_no_answer(void)

```
....
158.         if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2339
Status New

	Source	Destination
File	git@@git-v2.30.3-CVE-2020-5260-FP.c	git@@git-v2.30.3-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.30.3-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2340
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	159	159
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static int read_yes_no_answer(void)

```
....
159.        if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2341
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2020-5260-FP.c	git@@git-v2.30.8-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.30.8-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2342
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	159	159
Object	fgets	fgets

Code Snippet

File Name git@@git-v2.30.8-CVE-2021-21300-FP.c

Method static int read_yes_no_answer(void)

```
....
159.        if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2343
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c	git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet

File Name git@@git-v2.32.0-rc0-CVE-2020-5260-FP.c

Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2344
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	158	158
Object	fgets	fgets

Code Snippet

File Name	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method	static int read_yes_no_answer(void)

```
....
158.          if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2345
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2020-5260-FP.c	git@@git-v2.33.0-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet

File Name	git@@git-v2.33.0-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.          while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2346
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	158	158
Object	fgets	fgets

Code Snippet	
File Name	git@@git-v2.33.0-CVE-2021-21300-FP.c
Method	static int read_yes_no_answer(void)

```
....
158.          if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2347
Status	New

	Source	Destination
File	git@@git-v2.34.1-CVE-2020-5260-FP.c	git@@git-v2.34.1-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet	
File Name	git@@git-v2.34.1-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.          while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2348
Status	New

	Source	Destination
File	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	158	158
Object	fgets	fgets

Code Snippet	
File Name	git@@git-v2.34.1-CVE-2021-21300-FP.c
Method	static int read_yes_no_answer(void)

```
....
158.          if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2349
Status	New

	Source	Destination
File	git@@git-v2.37.0-CVE-2020-5260-FP.c	git@@git-v2.37.0-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.37.0-CVE-2020-5260-FP.c
Method static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2350
Status	New

	Source	Destination
File	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	161	161
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.37.0-CVE-2021-21300-FP.c
Method static int read_yes_no_answer(void)

```
....
161.        if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2351
Status	New

	Source	Destination

File	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet

File Name	git@@git-v2.38.0-rc2-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.         while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2352
Status	New

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	162	162
Object	fgets	fgets

Code Snippet

File Name	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method	static int read_yes_no_answer(void)

```
....
162.         if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2353
Status	New

	Source	Destination
File	git@@git-v2.39.5-CVE-2020-5260-FP.c	git@@git-v2.39.5-CVE-2020-5260-FP.c
Line	355	355
Object	fgets	fgets

Code Snippet

File Name	git@@git-v2.39.5-CVE-2020-5260-FP.c
Method	static int credential_read(struct credential *c)

```
....
355.        while (fgets(buf, 1024, stdin)) {
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2354
Status	New

	Source	Destination
File	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	162	162
Object	fgets	fgets

Code Snippet

File Name	git@@git-v2.39.5-CVE-2021-21300-FP.c
Method	static int read_yes_no_answer(void)

```
....
162.        if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2355
Status	New

	Source	Destination
File	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	169	169
Object	fgets	fgets

Code Snippet

File Name	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method	static int read_yes_no_answer(void)

```
....
169.        if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2356
Status	New

	Source	Destination
File	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	168	168
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.42.0-CVE-2021-21300-FP.c
Method static int read_yes_no_answer(void)

```
....
168.          if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2357
Status	New

	Source	Destination
File	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	168	168
Object	fgets	fgets

Code Snippet
File Name git@@git-v2.43.1-CVE-2021-21300-FP.c
Method static int read_yes_no_answer(void)

```
....
168.          if (fgets(answer, sizeof(answer), stdin)) {
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2358
Status	New

	Source	Destination

File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	666	666
Object	fscanf	fscanf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static void do_pidfile(const char *name)

```
....
666.                if (fscanf(f, "%ld", &pid) == 1)
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2359
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	556	556
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method int mingw_fgetc(FILE *stream)

```
....
556.                return fgetc(stream);
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2360
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	560	560
Object	fgetc	fgetc

Code Snippet

File Name	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method	int mingw_fgetc(FILE *stream)

```
....
560.                ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2361
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	569	569
Object	fgetc	fgetc

Code Snippet

File Name	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method	int mingw_fgetc(FILE *stream)

```
....
569.                return fgetc(stream);
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2362
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	573	573
Object	fgetc	fgetc

Code Snippet

File Name	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method	int mingw_fgetc(FILE *stream)

```
....
573.                ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2363
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	572	572
Object	fgetc	fgetc

Code Snippet

File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c

Method int mingw_fgetc(FILE *stream)

```
....
572.                return fgetc(stream);
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2364
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	576	576
Object	fgetc	fgetc

Code Snippet

File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c

Method int mingw_fgetc(FILE *stream)

```
....
576.                ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2365

Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	572	572
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method int mingw_fgetc(FILE *stream)

```
....
572.                return fgetc(stream);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2366
Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	576	576
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method int mingw_fgetc(FILE *stream)

```
....
576.                ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2367
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	575	575
Object	fgetc	fgetc

Code Snippet	
File Name	git@@git-v2.30.3-CVE-2021-21300-FP.c
Method	int mingw_fgetc(FILE *stream)

```
....
575.                 return fgetc(stream);
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2368
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	579	579
Object	fgetc	fgetc

Code Snippet	
File Name	git@@git-v2.30.3-CVE-2021-21300-FP.c
Method	int mingw_fgetc(FILE *stream)

```
....
579.                 ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2369
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	575	575
Object	fgetc	fgetc

Code Snippet	
File Name	git@@git-v2.30.8-CVE-2021-21300-FP.c
Method	int mingw_fgetc(FILE *stream)

```
....
575.                 return fgetc(stream);
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2370
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	579	579
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method int mingw_fgetc(FILE *stream)

```
....
579.                  ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2371
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	574	574
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method int mingw_fgetc(FILE *stream)

```
....
574.                  return fgetc(stream);
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2372
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	578	578
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method int mingw_fgetc(FILE *stream)

```
....
578.                  ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2373
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	595	595
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.33.0-CVE-2021-21300-FP.c
Method int mingw_fgetc(FILE *stream)

```
....
595.                  return fgetc(stream);
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2374
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	599	599
Object	fgetc	fgetc

Code Snippet

File Name	git@@git-v2.33.0-CVE-2021-21300-FP.c
Method	int mingw_fgetc(FILE *stream)

```
....
599.                ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2375
Status	New

	Source	Destination
File	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	595	595
Object	fgetc	fgetc

Code Snippet

File Name	git@@git-v2.34.1-CVE-2021-21300-FP.c
Method	int mingw_fgetc(FILE *stream)

```
....
595.                return fgetc(stream);
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2376
Status	New

	Source	Destination
File	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	599	599
Object	fgetc	fgetc

Code Snippet

File Name	git@@git-v2.34.1-CVE-2021-21300-FP.c
Method	int mingw_fgetc(FILE *stream)

```
....
599.                ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2377
Status	New

	Source	Destination
File	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	598	598
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.37.0-CVE-2021-21300-FP.c
Method int mingw_fgetc(FILE *stream)

```
....
598.                return fgetc(stream);
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2378
Status	New

	Source	Destination
File	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	602	602
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.37.0-CVE-2021-21300-FP.c
Method int mingw_fgetc(FILE *stream)

```
....
602.                ch = fgetc(stream);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2379
Status	New

	Source	Destination

File	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	599	599
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method int mingw_fgetc(FILE *stream)

```
....
599.            return fgetc(stream);
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2380
Status	New

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	603	603
Object	fgetc	fgetc

Code Snippet
File Name git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method int mingw_fgetc(FILE *stream)

```
....
603.            ch = fgetc(stream);
```

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=1000020&projectid=15&pathid=2696
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	724	724
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                                    snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2697
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	730	730
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                    snprintf(c, sizeof(c), "%02x",
data[i]);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2698

Status	New

The bgp_notify_receive method calls the snprintf function, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	1722	1722
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1722.                                     snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2699
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	1728	1728
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1728.                                     snprintf(c, sizeof(c), "%02x",
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=2700
Status	New

The bgp_route_refresh_receive method calls the sprintf function, at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	1870	1870
Object	sprintf	sprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1870.                         sprintf(name, "%s.%d.%d", peer->host, afi,
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2701
Status	New

The bgp_nlri_parse_flowspec method calls the snprintf function, at line 88 of FRRouting@@frr-frr-7.2.1-CVE-2023-41909-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	FRRouting@@frr-frr-7.2.1-CVE-2023-41909-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-41909-TP.c
Line	161	161
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-41909-TP.c
Method int bgp_nlri_parse_flowspec(struct peer *peer, struct attr *attr,

```
....
161.                          snprintf(ec_string, sizeof(ec_string),
```

Unchecked Return Value\Path 7:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2702
Status	New

The bgp_nlri_parse_flowspec method calls the snprintf function, at line 88 of FRRouting@@frr-frr-7.2.1-CVE-2023-41909-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	FRRouting@@frr-frr-7.2.1-CVE-2023-41909-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-41909-TP.c
Line	166	166
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2023-41909-TP.c
Method	int bgp_nlri_parse_flowspec(struct peer *peer, struct attr *attr,

```
....
166.                             snprintf(ec_string, sizeof(ec_string),
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2703
Status	New

The bgp_nlri_parse_flowspec method calls the snprintf function, at line 88 of FRRouting@@frr-frr-7.2.1-CVE-2023-41909-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	FRRouting@@frr-frr-7.2.1-CVE-2023-41909-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-41909-TP.c
Line	173	173
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.2.1-CVE-2023-41909-TP.c
Method	int bgp_nlri_parse_flowspec(struct peer *peer, struct attr *attr,

```
....
173.                       snprintf(local_string, sizeof(local_string),
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2704
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-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	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	724	724
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                              snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2705
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-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	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	730	730
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                              snprintf(c, sizeof(c), "%02x",
data[i]);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2706
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-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	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	1722	1722
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1722.                               snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2707
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-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	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	1728	1728
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1728.                               snprintf(c, sizeof(c), "%02x",
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2708
Status	New

The bgp_route_refresh_receive method calls the sprintf function, at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-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	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	1870	1870
Object	sprintf	sprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1870.                         sprintf(name, "%s.%d.%d", peer->host, afi,
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2709
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-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	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	724	724
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                              snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2710
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-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	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	730	730
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                    snprintf(c, sizeof(c), "%02x",
data[i]);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2711
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-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	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	1722	1722
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1722.                             snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2712
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1686 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-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	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	1728	1728
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1728.                             snprintf(c, sizeof(c), "%02x",
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2713
Status	New

The bgp_route_refresh_receive method calls the sprintf function, at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-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	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	1870	1870
Object	sprintf	sprintf

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c

Method	static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1870.                          sprintf(name, "%s.%d.%d", peer->host, afi,
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2714
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	724	724
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                              snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2715
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	730	730
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method	void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                    snprintf(c, sizeof(c), "%02x",
data[i]);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2716
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	1724	1724
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1724.                                   snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2717
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	1730	1730
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1730.                               snprintf(c, sizeof(c), "%02x",
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2718
Status	New

The bgp_route_refresh_receive method calls the sprintf function, at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	1874	1874
Object	sprintf	sprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1874.                          sprintf(name, "%s.%d.%d", peer->host, afi,
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2719
Status	New

The bgp_nlri_parse_flowspec method calls the snprintf function, at line 88 of FRRouting@@frr-frr-7.3.1-CVE-2023-41909-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	FRRouting@@frr-frr-7.3.1-CVE-2023-41909-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-41909-TP.c
Line	161	161

Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-41909-TP.c
Method	int bgp_nlri_parse_flowspec(struct peer *peer, struct attr *attr,

```
....
161.                          snprintf(ec_string, sizeof(ec_string),
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2720
Status	New

The bgp_nlri_parse_flowspec method calls the snprintf function, at line 88 of FRRouting@@frr-frr-7.3.1-CVE-2023-41909-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	FRRouting@@frr-frr-7.3.1-CVE-2023-41909-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-41909-TP.c
Line	166	166
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-41909-TP.c
Method	int bgp_nlri_parse_flowspec(struct peer *peer, struct attr *attr,

```
....
166.                                 snprintf(ec_string, sizeof(ec_string),
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2721
Status	New

The bgp_nlri_parse_flowspec method calls the snprintf function, at line 88 of FRRouting@@frr-frr-7.3.1-CVE-2023-41909-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	FRRouting@@frr-frr-7.3.1-CVE-2023-41909-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-41909-TP.c

Line	173	173
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-41909-TP.c
Method int bgp_nlri_parse_flowspec(struct peer *peer, struct attr *attr,

```
....
173.                    snprintf(local_string, sizeof(local_string),
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2722
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-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	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	724	724
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                            snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2723
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-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	FRRouting@@frr-frr-7.3.1-CVE-2023-	FRRouting@@frr-frr-7.3.1-CVE-2023-

	47234-TP.c	47234-TP.c
Line	730	730
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                    snprintf(c, sizeof(c), "%02x",
data[i]);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2724
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-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	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	1724	1724
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1724.                                   snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2725
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-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	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	1730	1730
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1730.                               snprintf(c, sizeof(c), "%02x",
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2726
Status	New

The bgp_route_refresh_receive method calls the sprintf function, at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-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	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	1874	1874
Object	sprintf	sprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1874.                          sprintf(name, "%s.%d.%d", peer->host, afi,
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2727
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-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	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	724	724
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
724.                                snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2728
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 662 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-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	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	730	730
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
730.                                snprintf(c, sizeof(c), "%02x",
data[i]);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2729
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-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	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	1724	1724
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1724.                                   snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2730
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1688 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-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	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	1730	1730
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1730.                                   snprintf(c, sizeof(c), "%02x",
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2731
Status	New

The bgp_route_refresh_receive method calls the sprintf function, at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-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	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	1874	1874
Object	sprintf	sprintf

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1874.                         sprintf(name, "%s.%d.%d", peer->host, afi,
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2732
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	742	742
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
742.                              snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2733

Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	750	750
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
750.                                    snprintf(c, sizeof(c), "%02x",
data[i]);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2734
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	1832	1832
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Method static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1832.                                   snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 40:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2735
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	1840	1840
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1840.                                snprintf(c, sizeof(c), "%02x",
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2736
Status	New

The bgp_route_refresh_receive method calls the snprintf function, at line 1883 of FRRouting@@frr-frr-7.5.1-CVE-2022-37032-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	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Line	1988	1988
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2022-37032-TP.c
Method	static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1988.                           snprintf(name, sizeof(name), "%s.%d.%d",
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2737
Status	New

The pid_is_exec method calls the snprintf function, at line 600 of FRRouting@@frr-frr-7.5.1-CVE-2023-46752-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	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	605	605
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static int pid_is_exec(pid_t pid, const struct stat *esb)

```
....
605.         snprintf(buf, sizeof(buf), "/proc/%ld/exe", (long)pid);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2738
Status	New

The pid_is_user method calls the snprintf function, at line 612 of FRRouting@@frr-frr-7.5.1-CVE-2023-46752-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	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	617	617
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static int pid_is_user(pid_t pid, uid_t uid)

```
....
617.         snprintf(buf, sizeof(buf), "/proc/%ld", (long)pid);
```

Unchecked Return Value\Path 44:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2739
Status	New

The pid_is_cmd method calls the snprintf function, at line 624 of FRRouting@@frr-frr-7.5.1-CVE-2023-46752-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	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	630	630
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method	static int pid_is_cmd(pid_t pid, const char *name)

```
....
630.            snprintf(buf, sizeof(buf), "/proc/%ld/stat", (long)pid);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2740
Status	New

The run_stop_schedule method calls the sprintf function, at line 755 of FRRouting@@frr-frr-7.5.1-CVE-2023-46752-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	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	773	773
Object	sprintf	sprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method	static int run_stop_schedule(void)

```
....
773.                    sprintf(what_stop, "process in pidfile `%.200s'",
pidfile);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2741
Status	New

The run_stop_schedule method calls the sprintf function, at line 755 of FRRouting@@frr-frr-7.5.1-CVE-2023-46752-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	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	775	775
Object	sprintf	sprintf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static int run_stop_schedule(void)

```
....
775.            sprintf(what_stop, "process(es) owned by `%.200s'",
userspec);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2742
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Line	742	742
Object	snprintf	snprintf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
742.                            snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2743
Status	New

The bgp_notify_send_with_data method calls the snprintf function, at line 680 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Line	750	750
Object	snprintf	snprintf

Code Snippet

File Name FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c

Method void bgp_notify_send_with_data(struct peer *peer, uint8_t code,

```
....
750.                            snprintf(c, sizeof(c), "%02x",
data[i]);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2744
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Line	1832	1832
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1832.                                   snprintf(c, sizeof(c), " %02x",
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2745
Status	New

The bgp_notify_receive method calls the snprintf function, at line 1796 of FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Line	1840	1840
Object	snprintf	snprintf

Code Snippet

File Name	FRRouting@@frr-frr-7.5.1-CVE-2023-47234-FP.c
Method	static int bgp_notify_receive(struct peer *peer, bgp_size_t size)

```
....
1840.                                   snprintf(c, sizeof(c), "%02x",
```

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=1000020&projectid=15&pathid=2595
Status	New

	Source	Destination

File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	631	631
Object	f	f

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static int pid_is_cmd(pid_t pid, const char *name)

```
....
631.         f = fopen(buf, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2596
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	664	664
Object	f	f

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static void do_pidfile(const char *name)

```
....
664.         f = fopen(name, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2597
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	593	593
Object	file	file

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
593.         file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2598
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	606	606
Object	file	file

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
606.         file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2599
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	609	609
Object	file	file

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
609.         file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2600
Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	609	609
Object	file	file

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
609.         file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2601
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	612	612
Object	file	file

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
612.         file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2602
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	612	612
Object	file	file

Code Snippet

File Name git@@git-v2.30.8-CVE-2021-21300-FP.c

Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
612.        file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2603
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	611	611
Object	file	file

Code Snippet

File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c

Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
611.        file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2604
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	632	632
Object	file	file

Code Snippet

File Name	git@@git-v2.33.0-CVE-2021-21300-FP.c
Method	FILE *mingw_fopen (const char *filename, const char *otype)

```
....
632.          file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2605
Status	New

	Source	Destination
File	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	632	632
Object	file	file

Code Snippet

File Name	git@@git-v2.34.1-CVE-2021-21300-FP.c
Method	FILE *mingw_fopen (const char *filename, const char *otype)

```
....
632.          file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2606
Status	New

	Source	Destination
File	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	635	635
Object	file	file

Code Snippet

File Name	git@@git-v2.37.0-CVE-2021-21300-FP.c
Method	FILE *mingw_fopen (const char *filename, const char *otype)

```
....
635.          file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2607
Status	New

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	636	636
Object	file	file

Code Snippet

File Name	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method	FILE *mingw_fopen (const char *filename, const char *otype)

```
....
636.         file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2608
Status	New

	Source	Destination
File	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	639	639
Object	file	file

Code Snippet

File Name	git@@git-v2.39.5-CVE-2021-21300-FP.c
Method	FILE *mingw_fopen (const char *filename, const char *otype)

```
....
639.         file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2609
Status	New

	Source	Destination
File	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	646	646
Object	file	file

Code Snippet
File Name git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
646.         file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2610
Status	New

	Source	Destination
File	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	646	646
Object	file	file

Code Snippet
File Name git@@git-v2.42.0-CVE-2021-21300-FP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
646.         file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2611
Status	New

	Source	Destination
File	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	648	648
Object	file	file

Code Snippet
File Name git@@git-v2.43.1-CVE-2021-21300-FP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
648.         file = _wfopen(wfilename, wotype);
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2612
Status New

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	1050	1050
Object	pidf	pidf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method int main(int argc, char **argv)

```
....
1050.             FILE *pidf = fopen(pidfile, "w");
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2613
Status New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	460	460
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static int mingw_open_append(wchar_t const *wfilename, int oflags, ...)

```
....
460.         handle = CreateFileW(wfilename, FILE_APPEND_DATA,
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2614
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	1061	1061
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method char *mingw_getcwd(char *pointer, int len)

```
....
1061.               HANDLE hnd = CreateFileW(cwd, 0,
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2615
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	1499	1499
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1499.         cons = CreateFileW(L"CONOUT$", GENERIC_WRITE,
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=2616
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	2735	2735
Object	CreateFileW	CreateFileW

Code Snippet

File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c

Method static void maybe_redirect_std_handle(const wchar_t *key, DWORD std_id, int fd,

```
....
2735.       handle = CreateFileW(buf, desired_access, 0, NULL,
create_flag,
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2617
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	460	460
Object	CreateFileW	CreateFileW

Code Snippet

File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c

Method static int mingw_open_append(wchar_t const *wfilename, int oflags, ...)

```
....
460.        handle = CreateFileW(wfilename, FILE_APPEND_DATA,
```

Incorrect Permission Assignment For Critical Resources\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2618
Status	New

	Source	Destination

File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	1083	1083
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method char *mingw_getcwd(char *pointer, int len)

```
....
1083.                HANDLE hnd = CreateFileW(cwd, 0,
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2619
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	1522	1522
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1522.         cons = CreateFileW(L"CONOUT$", GENERIC_WRITE,
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2620
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	2785	2785
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method static void maybe_redirect_std_handle(const wchar_t *key, DWORD std_id, int fd,

```
....
2785.        handle = CreateFileW(buf, desired_access, 0, NULL,
create_flag,
```

Incorrect Permission Assignment For Critical Resources\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2621
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	463	463
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method static int mingw_open_append(wchar_t const *wfilename, int oflags, ...)

```
....
463.        handle = CreateFileW(wfilename, FILE_APPEND_DATA,
```

Incorrect Permission Assignment For Critical Resources\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2622
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	1086	1086
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method char *mingw_getcwd(char *pointer, int len)

```
....
1086.              HANDLE hnd = CreateFileW(cwd, 0,
```

Incorrect Permission Assignment For Critical Resources\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2623
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	1525	1525
Object	CreateFileW	CreateFileW

Code Snippet

File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c

Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1525.        cons = CreateFileW(L"CONOUT$", GENERIC_WRITE,
```

Incorrect Permission Assignment For Critical Resources\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2624
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	2788	2788
Object	CreateFileW	CreateFileW

Code Snippet

File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c

Method static void maybe_redirect_std_handle(const wchar_t *key, DWORD std_id, int fd,

```
....
2788.        handle = CreateFileW(buf, desired_access, 0, NULL,
create_flag,
```

Incorrect Permission Assignment For Critical Resources\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2625
Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	463	463
Object	CreateFileW	CreateFileW

Code Snippet

File Name git@@git-v2.30.1-CVE-2021-21300-TP.c

Method static int mingw_open_append(wchar_t const *wfilename, int oflags, ...)

```
....
463.          handle = CreateFileW(wfilename, FILE_APPEND_DATA,
```

Incorrect Permission Assignment For Critical Resources\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2626
Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	1086	1086
Object	CreateFileW	CreateFileW

Code Snippet

File Name git@@git-v2.30.1-CVE-2021-21300-TP.c

Method char *mingw_getcwd(char *pointer, int len)

```
....
1086.                HANDLE hnd = CreateFileW(cwd, 0,
```

Incorrect Permission Assignment For Critical Resources\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2627
Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	1525	1525
Object	CreateFileW	CreateFileW

Code Snippet

File Name	git@@git-v2.30.1-CVE-2021-21300-TP.c
Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1525.        cons = CreateFileW(L"CONOUT$", GENERIC_WRITE,
```

Incorrect Permission Assignment For Critical Resources\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2628
Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	2788	2788
Object	CreateFileW	CreateFileW

Code Snippet

File Name	git@@git-v2.30.1-CVE-2021-21300-TP.c
Method	static void maybe_redirect_std_handle(const wchar_t *key, DWORD std_id, int fd,

```
....
2788.        handle = CreateFileW(buf, desired_access, 0, NULL,
create_flag,
```

Incorrect Permission Assignment For Critical Resources\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2629
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	466	466
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static int mingw_open_append(wchar_t const *wfilename, int oflags, ...)

```
....
466.          handle = CreateFileW(wfilename, FILE_APPEND_DATA,
```

Incorrect Permission Assignment For Critical Resources\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2630
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	1091	1091
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method char *mingw_getcwd(char *pointer, int len)

```
....
1091.                HANDLE hnd = CreateFileW(cwd, 0,
```

Incorrect Permission Assignment For Critical Resources\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2631
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	1530	1530
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1530.          cons = CreateFileW(L"CONOUT$", GENERIC_WRITE,
```

Incorrect Permission Assignment For Critical Resources\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2632
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	2879	2879
Object	CreateFileW	CreateFileW

Code Snippet

File Name git@@git-v2.30.3-CVE-2021-21300-FP.c

Method static void maybe_redirect_std_handle(const wchar_t *key, DWORD std_id, int fd,

```
....
2879.         handle = CreateFileW(buf, desired_access, 0, NULL,
create_flag,
```

Incorrect Permission Assignment For Critical Resources\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2633
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	466	466
Object	CreateFileW	CreateFileW

Code Snippet

File Name git@@git-v2.30.8-CVE-2021-21300-FP.c

Method static int mingw_open_append(wchar_t const *wfilename, int oflags, ...)

```
....
466.          handle = CreateFileW(wfilename, FILE_APPEND_DATA,
```

Incorrect Permission Assignment For Critical Resources\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2634

Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	1091	1091
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method char *mingw_getcwd(char *pointer, int len)

```
....
1091.            HANDLE hnd = CreateFileW(cwd, 0,
```

Incorrect Permission Assignment For Critical Resources\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2635
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	1530	1530
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1530.        cons = CreateFileW(L"CONOUT$", GENERIC_WRITE,
```

Incorrect Permission Assignment For Critical Resources\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2636
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	2879	2879

Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method static void maybe_redirect_std_handle(const wchar_t *key, DWORD std_id, int fd,

```
....
2879.        handle = CreateFileW(buf, desired_access, 0, NULL,
create_flag,
```

Incorrect Permission Assignment For Critical Resources\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2637
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	465	465
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method static int mingw_open_append(wchar_t const *wfilename, int oflags, ...)

```
....
465.        handle = CreateFileW(wfilename, FILE_APPEND_DATA,
```

Incorrect Permission Assignment For Critical Resources\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2638
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	1090	1090
Object	CreateFileW	CreateFileW

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c

Method	char *mingw_getcwd(char *pointer, int len)

```
....
1090.            HANDLE hnd = CreateFileW(cwd, 0,
```

Incorrect Permission Assignment For Critical Resources\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2639
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	1529	1529
Object	CreateFileW	CreateFileW

Code Snippet

File Name	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1529.        cons = CreateFileW(L"CONOUT$", GENERIC_WRITE,
```

Incorrect Permission Assignment For Critical Resources\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2640
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	2792	2792
Object	CreateFileW	CreateFileW

Code Snippet

File Name	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method	static void maybe_redirect_std_handle(const wchar_t *key, DWORD std_id, int fd,

```
....
2792.        handle = CreateFileW(buf, desired_access, 0, NULL,
create_flag,
```

Incorrect Permission Assignment For Critical Resources\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2641
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	486	486
Object	CreateFileW	CreateFileW

Code Snippet

File Name	git@@git-v2.33.0-CVE-2021-21300-FP.c
Method	static int mingw_open_append(wchar_t const *wfilename, int oflags, ...)

```
....
486.        handle = CreateFileW(wfilename, FILE_APPEND_DATA,
```

Incorrect Permission Assignment For Critical Resources\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2642
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	1111	1111
Object	CreateFileW	CreateFileW

Code Snippet

File Name	git@@git-v2.33.0-CVE-2021-21300-FP.c
Method	char *mingw_getcwd(char *pointer, int len)

```
....
1111.            HANDLE hnd = CreateFileW(cwd, 0,
```

Incorrect Permission Assignment For Critical Resources\Path 49:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2643
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	1550	1550
Object	CreateFileW	CreateFileW

Code Snippet

File Name	git@@git-v2.33.0-CVE-2021-21300-FP.c
Method	static pid_t mingw_spawnve_fd(const char *cmd, const char **argv, char **deltaenv,

```
....
1550.        cons = CreateFileW(L"CONOUT$", GENERIC_WRITE,
```

Incorrect Permission Assignment For Critical Resources\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2644
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	2813	2813
Object	CreateFileW	CreateFileW

Code Snippet

File Name	git@@git-v2.33.0-CVE-2021-21300-FP.c
Method	static void maybe_redirect_std_handle(const wchar_t *key, DWORD std_id, int fd,

```
....
2813.        handle = CreateFileW(buf, desired_access, 0, NULL,
create_flag,
```

Unchecked Array Index

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unchecked Array Index\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3443
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	90	90
Object	p	p

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_parse_message(stun_msg_t *msg)

```
....
90.     msg->stun_hdr.msg_type = get16(p, 0);
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3444
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	90	90
Object	p	p

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_parse_message(stun_msg_t *msg)

```
....
90.     msg->stun_hdr.msg_type = get16(p, 0);
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3445
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	91	91
Object	p	p

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_parse_message(stun_msg_t *msg)

```
....
91.    msg->stun_hdr.msg_len = get16(p, 2);
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3446
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	91	91
Object	p	p

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method	int stun_parse_message(stun_msg_t *msg)

```
....
91.    msg->stun_hdr.msg_len = get16(p, 2);
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3447
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	90	90

Object	p	p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_parse_message(stun_msg_t *msg)

```
....
90.     msg->stun_hdr.msg_type = get16(p, 0);
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3448
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	90	90
Object	p	p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_parse_message(stun_msg_t *msg)

```
....
90.     msg->stun_hdr.msg_type = get16(p, 0);
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3449
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	91	91
Object	p	p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_parse_message(stun_msg_t *msg)

```
....
91.     msg->stun_hdr.msg_len = get16(p, 2);
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3450
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	91	91
Object	p	p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method int stun_parse_message(stun_msg_t *msg)

```
....
91.     msg->stun_hdr.msg_len = get16(p, 2);
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3451
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	90	90
Object	p	p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method int stun_parse_message(stun_msg_t *msg)

```
....
90.     msg->stun_hdr.msg_type = get16(p, 0);
```

Unchecked Array Index\Path 10:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3452
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	90	90
Object	p	p

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method	int stun_parse_message(stun_msg_t *msg)

```
....
90.     msg->stun_hdr.msg_type = get16(p, 0);
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3453
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	91	91
Object	p	p

Code Snippet

File Name	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method	int stun_parse_message(stun_msg_t *msg)

```
....
91.     msg->stun_hdr.msg_len = get16(p, 2);
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3454
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	91	91
Object	p	p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method int stun_parse_message(stun_msg_t *msg)

```
....
91.     msg->stun_hdr.msg_len = get16(p, 2);
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3455
Status	New

	Source	Destination
File	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Line	2381	2381
Object	SIGNAL_DEVICE_ADDED	SIGNAL_DEVICE_ADDED

Code Snippet
File Name fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Method fu_plugin_class_init(FuPluginClass *klass)

```
....
2381.       signals[SIGNAL_DEVICE_ADDED] = g_signal_new("device-added",
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3456
Status	New

	Source	Destination
File	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Line	2400	2400

Object	SIGNAL_DEVICE_REMOVED	SIGNAL_DEVICE_REMOVED

Code Snippet
File Name fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Method fu_plugin_class_init(FuPluginClass *klass)

```
....
2400.        signals[SIGNAL_DEVICE_REMOVED] =
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3457
Status	New

	Source	Destination
File	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Line	2420	2420
Object	SIGNAL_DEVICE_REGISTER	SIGNAL_DEVICE_REGISTER

Code Snippet
File Name fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Method fu_plugin_class_init(FuPluginClass *klass)

```
....
2420.        signals[SIGNAL_DEVICE_REGISTER] =
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3458
Status	New

	Source	Destination
File	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Line	2443	2443
Object	SIGNAL_CHECK_SUPPORTED	SIGNAL_CHECK_SUPPORTED

Code Snippet
File Name fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Method fu_plugin_class_init(FuPluginClass *klass)

```
....
2443.        signals[SIGNAL_CHECK_SUPPORTED] =
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3459
Status	New

	Source	Destination
File	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Line	2454	2454
Object	SIGNAL_RULES_CHANGED	SIGNAL_RULES_CHANGED

Code Snippet

File Name	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Method	fu_plugin_class_init(FuPluginClass *klass)

```
....
2454.        signals[SIGNAL_RULES_CHANGED] = g_signal_new("rules-
changed",
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3460
Status	New

	Source	Destination
File	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Line	2472	2472
Object	SIGNAL_CONFIG_CHANGED	SIGNAL_CONFIG_CHANGED

Code Snippet

File Name	fwupd@@fwupd-1.7.4-CVE-2022-3287-TP.c
Method	fu_plugin_class_init(FuPluginClass *klass)

```
....
2472.        signals[SIGNAL_CONFIG_CHANGED] =
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3461
Status	New

	Source	Destination
File	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Line	2391	2391
Object	SIGNAL_DEVICE_ADDED	SIGNAL_DEVICE_ADDED

Code Snippet

File Name	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Method	fu_plugin_class_init(FuPluginClass *klass)

```
....
2391.        signals[SIGNAL_DEVICE_ADDED] = g_signal_new("device-added",
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3462
Status	New

	Source	Destination
File	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Line	2410	2410
Object	SIGNAL_DEVICE_REMOVED	SIGNAL_DEVICE_REMOVED

Code Snippet

File Name	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Method	fu_plugin_class_init(FuPluginClass *klass)

```
....
2410.        signals[SIGNAL_DEVICE_REMOVED] =
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3463
Status	New

	Source	Destination
File	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Line	2430	2430
Object	SIGNAL_DEVICE_REGISTER	SIGNAL_DEVICE_REGISTER

Code Snippet
File Name fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Method fu_plugin_class_init(FuPluginClass *klass)

```
....
2430.        signals[SIGNAL_DEVICE_REGISTER] =
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3464
Status	New

	Source	Destination
File	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Line	2453	2453
Object	SIGNAL_CHECK_SUPPORTED	SIGNAL_CHECK_SUPPORTED

Code Snippet
File Name fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Method fu_plugin_class_init(FuPluginClass *klass)

```
....
2453.        signals[SIGNAL_CHECK_SUPPORTED] =
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3465
Status	New

	Source	Destination
File	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Line	2464	2464

Object	SIGNAL_RULES_CHANGED	SIGNAL_RULES_CHANGED

Code Snippet
File Name fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Method fu_plugin_class_init(FuPluginClass *klass)

```
....
2464.       signals[SIGNAL_RULES_CHANGED] = g_signal_new("rules-
changed",
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3466
Status	New

	Source	Destination
File	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c	fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Line	2482	2482
Object	SIGNAL_CONFIG_CHANGED	SIGNAL_CONFIG_CHANGED

Code Snippet
File Name fwupd@@fwupd-1.8.0-CVE-2022-3287-TP.c
Method fu_plugin_class_init(FuPluginClass *klass)

```
....
2482.       signals[SIGNAL_CONFIG_CHANGED] =
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3467
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c
Line	292	292
Object	i	i

Code Snippet
File Name github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c
Method static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
292.        alignments[i] = 'c';
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3468
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c
Line	294	294
Object	i	i

Code Snippet

File Name	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c
Method	static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
294.        alignments[i] = 'l';
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3469
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c
Line	296	296
Object	i	i

Code Snippet

File Name	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-37463-TP.c
Method	static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
296.        alignments[i] = 'r';
```

Unchecked Array Index\Path 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3470
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c
Line	312	312
Object	i	i

Code Snippet

File Name github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c

Method static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
312.         alignments[i] = 'c';
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3471
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c
Line	314	314
Object	i	i

Code Snippet

File Name github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c

Method static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
314.         alignments[i] = 'l';
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3472
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c
Line	316	316
Object	i	i

Code Snippet
File Name github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-37463-TP.c
Method static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
316.         alignments[i] = 'r';
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3473
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c
Line	312	312
Object	i	i

Code Snippet
File Name github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c
Method static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
312.         alignments[i] = 'c';
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3474
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c
Line	314	314

Object	i	i

Code Snippet
File Name github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c
Method static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
314.          alignments[i] = 'l';
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3475
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c
Line	316	316
Object	i	i

Code Snippet
File Name github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-37463-TP.c
Method static cmark_node *try_opening_table_header(cmark_syntax_extension *self,

```
....
316.          alignments[i] = 'r';
```

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=1000020&projectid=15&pathid=3410
Status	New

The main method in FRRouting@@frr-frr-7.5.1-CVE-2023-46752-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	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c

Line	1050	1050
Object	fopen	fopen

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method int main(int argc, char **argv)

```
....
1050.                FILE *pidf = fopen(pidfile, "w");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3411
Status	New

The pid_is_cmd method in FRRouting@@frr-frr-7.5.1-CVE-2023-46752-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	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	631	631
Object	fopen	fopen

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static int pid_is_cmd(pid_t pid, const char *name)

```
....
631.         f = fopen(buf, "r");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3412
Status	New

The do_pidfile method in FRRouting@@frr-frr-7.5.1-CVE-2023-46752-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	FRRouting@@frr-frr-7.5.1-CVE-2023-	FRRouting@@frr-frr-7.5.1-CVE-2023-

	46752-TP.c	46752-TP.c
Line	664	664
Object	fopen	fopen

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static void do_pidfile(const char *name)

```
....
664.         f = fopen(name, "r");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3413
Status	New

The main method in FRRouting@@frr-frr-7.5.1-CVE-2023-46752-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	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	1026	1026
Object	open	open

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method int main(int argc, char **argv)

```
....
1026.             fd = open("/dev/tty", O_RDWR);
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3414
Status	New

The main method in FRRouting@@frr-frr-7.5.1-CVE-2023-46752-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	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	1036	1036
Object	open	open

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method int main(int argc, char **argv)

```
....
1036.                fd = open("/dev/null", O_RDWR); /* stdin */
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3415
Status	New

The mkstemp method in git@@git-v2.26.0-rc1-CVE-2021-21300-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	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	997	997
Object	open	open

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method int mkstemp(char *template)

```
....
997.         return open(filename, O_RDWR | O_CREAT, 0600);
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3416
Status	New

The *parse_interpreter method in git@@git-v2.26.0-rc1-CVE-2021-21300-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	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	1187	1187
Object	open	open

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1187.        fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3417
Status	New

The mkstemp method in git@@git-v2.28.0-rc0-CVE-2021-21300-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	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	1019	1019
Object	open	open

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method int mkstemp(char *template)

```
....
1019.        return open(filename, O_RDWR | O_CREAT, 0600);
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3418
Status	New

The *parse_interpreter method in git@@git-v2.28.0-rc0-CVE-2021-21300-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	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	1209	1209
Object	open	open

Code Snippet
File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1209.       fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3419
Status	New

The mkstemp method in git@@git-v2.29.0-rc2-CVE-2021-21300-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	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	1022	1022
Object	open	open

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method int mkstemp(char *template)

```
....
1022.       return open(filename, O_RDWR | O_CREAT, 0600);
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3420
Status	New

The *parse_interpreter method in git@@git-v2.29.0-rc2-CVE-2021-21300-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	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	1212	1212
Object	open	open

Code Snippet
File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1212.        fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3421
Status	New

The mkstemp method in git@@git-v2.30.1-CVE-2021-21300-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	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	1022	1022
Object	open	open

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method int mkstemp(char *template)

```
....
1022.        return open(filename, O_RDWR | O_CREAT, 0600);
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3422
Status	New

The *parse_interpreter method in git@@git-v2.30.1-CVE-2021-21300-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	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	1212	1212
Object	open	open

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1212.        fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3423
Status	New

The mkstemp method in git@@git-v2.30.3-CVE-2021-21300-FP.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	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	1025	1025
Object	open	open

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method int mkstemp(char *template)

```
....
1025.        return open(filename, O_RDWR | O_CREAT, 0600);
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3424
Status	New

The *parse_interpreter method in git@@git-v2.30.3-CVE-2021-21300-FP.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	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	1217	1217
Object	open	open

Code Snippet
File Name　　git@@git-v2.30.3-CVE-2021-21300-FP.c
Method　　static const char *parse_interpreter(const char *cmd)

```
....
1217.        fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3425
Status	New

The mkstemp method in git@@git-v2.30.8-CVE-2021-21300-FP.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	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	1025	1025
Object	open	open

Code Snippet
File Name　　git@@git-v2.30.8-CVE-2021-21300-FP.c
Method　　int mkstemp(char *template)

```
....
1025.        return open(filename, O_RDWR | O_CREAT, 0600);
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3426
Status	New

The *parse_interpreter method in git@@git-v2.30.8-CVE-2021-21300-FP.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	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	1217	1217
Object	open	open

Code Snippet
File Name	git@@git-v2.30.8-CVE-2021-21300-FP.c
Method	static const char *parse_interpreter(const char *cmd)

```
....
1217.        fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3427
Status	New

The mkstemp method in git@@git-v2.32.0-rc0-CVE-2021-21300-FP.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	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	1026	1026
Object	open	open

Code Snippet
File Name	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method	int mkstemp(char *template)

```
....
1026.        return open(filename, O_RDWR | O_CREAT, 0600);
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3428
Status	New

The *parse_interpreter method in git@@git-v2.32.0-rc0-CVE-2021-21300-FP.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	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	1216	1216
Object	open	open

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1216.           fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3429
Status	New

The mkstemp method in git@@git-v2.33.0-CVE-2021-21300-FP.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	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	1047	1047
Object	open	open

Code Snippet
File Name git@@git-v2.33.0-CVE-2021-21300-FP.c
Method int mkstemp(char *template)

```
....
1047.           return open(filename, O_RDWR | O_CREAT, 0600);
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3430
Status	New

The *parse_interpreter method in git@@git-v2.33.0-CVE-2021-21300-FP.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	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	1237	1237
Object	open	open

Code Snippet
File Name git@@git-v2.33.0-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1237.         fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3431
Status	New

The mkstemp method in git@@git-v2.34.1-CVE-2021-21300-FP.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	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	1047	1047
Object	open	open

Code Snippet
File Name git@@git-v2.34.1-CVE-2021-21300-FP.c
Method int mkstemp(char *template)

```
....
1047.         return open(filename, O_RDWR | O_CREAT, 0600);
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3432
Status	New

The *parse_interpreter method in git@@git-v2.34.1-CVE-2021-21300-FP.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	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	1237	1237
Object	open	open

Code Snippet

File Name	git@@git-v2.34.1-CVE-2021-21300-FP.c
Method	static const char *parse_interpreter(const char *cmd)

```
....
1237.       fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3433
Status	New

The mkstemp method in git@@git-v2.37.0-CVE-2021-21300-FP.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	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	1065	1065
Object	open	open

Code Snippet

File Name	git@@git-v2.37.0-CVE-2021-21300-FP.c
Method	int mkstemp(char *template)

```
....
1065.       return open(filename, O_RDWR | O_CREAT, 0600);
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3434
Status	New

The *parse_interpreter method in git@@git-v2.37.0-CVE-2021-21300-FP.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	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	1261	1261
Object	open	open

Code Snippet
File Name git@@git-v2.37.0-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1261.        fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3435
Status	New

The *parse_interpreter method in git@@git-v2.38.0-rc2-CVE-2021-21300-FP.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	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	1259	1259
Object	open	open

Code Snippet
File Name git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1259.        fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3436
Status	New

The *parse_interpreter method in git@@git-v2.39.5-CVE-2021-21300-FP.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	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	1262	1262
Object	open	open

Code Snippet
File Name git@@git-v2.39.5-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1262.        fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3437
Status	New

The *parse_interpreter method in git@@git-v2.41.0-rc0-CVE-2021-21300-FP.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	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	1269	1269
Object	open	open

Code Snippet
File Name git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1269.        fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3438
Status	New

The *parse_interpreter method in git@@git-v2.42.0-CVE-2021-21300-FP.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	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	1269	1269
Object	open	open

Code Snippet
File Name git@@git-v2.42.0-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1269.        fd = open(cmd, O_RDONLY);
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3439
Status	New

The *parse_interpreter method in git@@git-v2.43.1-CVE-2021-21300-FP.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	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	1271	1271
Object	open	open

Code Snippet
File Name git@@git-v2.43.1-CVE-2021-21300-FP.c
Method static const char *parse_interpreter(const char *cmd)

```
....
1271.        fd = open(cmd, O_RDONLY);
```

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=1000020&projectid=15&pathid=1774
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c at line 1463 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	1570	1570
Object	<=	<=

Code Snippet

File Name	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method	ft_var_load_gvar(TT_Face face)

```
....
1570.         for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1775
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c at line 1463 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	1600	1600
Object	<=	<=

Code Snippet

File Name	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method	ft_var_load_gvar(TT_Face face)

```
....
1600.         for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1776
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c at line 3563 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Line	3579	3579
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-10-2-CVE-2023-2004-TP.c
Method tt_delta_interpolate(int p1,

```
....
3579.       for ( i = 0; i <= 1; i++ )
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1777
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c at line 1463 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	1570	1570
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method ft_var_load_gvar(TT_Face face)

```
....
1570.         for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=1778
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c at line 1463 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	1600	1600
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method ft_var_load_gvar(TT_Face face)

```
....
1600.         for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1779
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c at line 3563 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Line	3579	3579
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-10-3-CVE-2023-2004-TP.c
Method tt_delta_interpolate(int p1,

```
....
3579.       for ( i = 0; i <= 1; i++ )
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1780

Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c at line 1473 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	1581	1581
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method ft_var_load_gvar(TT_Face face)

```
....
1581.         for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1781
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c at line 1473 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	1611	1611
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method ft_var_load_gvar(TT_Face face)

```
....
1611.         for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1782
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c at line 3575 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Line	3591	3591
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-11-0-CVE-2023-2004-TP.c
Method tt_delta_interpolate(int p1,

```
....
3591.        for ( i = 0; i <= 1; i++ )
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1783
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c at line 1545 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	1653	1653
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method ft_var_load_gvar(TT_Face face)

```
....
1653.        for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1784
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c at line 1545 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	1683	1683
Object	<=	<=

Code Snippet

File Name	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method	ft_var_load_gvar(TT_Face face)

```
....
1683.         for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1785
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c at line 3659 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Line	3675	3675
Object	<=	<=

Code Snippet

File Name	freetype@@freetype-VER-2-11-1-CVE-2023-2004-TP.c
Method	tt_delta_interpolate(int p1,

```
....
3675.       for ( i = 0; i <= 1; i++ )
```

Potential Off by One Error in Loops\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1786
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c at line 1538 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	1646	1646
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method ft_var_load_gvar(TT_Face face)

```
....
1646.         for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1787
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c at line 1538 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	1676	1676
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method ft_var_load_gvar(TT_Face face)

```
....
1676.         for ( i = 0; i <= gvar_head.glyphCount; i++ )
```

Potential Off by One Error in Loops\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1788
Status	New

The buffer allocated by <= in freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c at line 3651 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c	freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Line	3667	3667
Object	<=	<=

Code Snippet
File Name freetype@@freetype-VER-2-12-0-CVE-2023-2004-TP.c
Method tt_delta_interpolate(int p1,

```
....
3667.       for ( i = 0; i <= 1; i++ )
```

Potential Off by One Error in Loops\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1789
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-7.2.1-CVE-2023-46753-TP.c at line 1025 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-46753-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-46753-TP.c
Line	1035	1035
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-46753-TP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1035.        for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1790
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-7.2.1-CVE-2023-47235-TP.c at line 1025 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-47235-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47235-TP.c
Line	1035	1035
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47235-TP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1035.          for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1791
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-7.2.1-CVE-2024-31948-TP.c at line 1025 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2024-31948-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31948-TP.c
Line	1035	1035
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2024-31948-TP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1035.          for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1792
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-7.5.1-CVE-2023-46753-FP.c at line 1255 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46753-FP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46753-FP.c
Line	1265	1265
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46753-FP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1265.        for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1793
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-7.5.1-CVE-2024-31948-TP.c at line 1255 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2024-31948-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2024-31948-TP.c
Line	1265	1265
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2024-31948-TP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1265.        for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1794
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-8.0.1-CVE-2023-46753-TP.c at line 1308 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-46753-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-46753-TP.c
Line	1318	1318
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-46753-TP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1318.         for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1795
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-8.0.1-CVE-2023-47235-TP.c at line 1308 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2023-47235-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2023-47235-TP.c
Line	1318	1318
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2023-47235-TP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1318.         for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1796
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-8.0.1-CVE-2024-31948-TP.c at line 1308 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-8.0.1-CVE-2024-31948-TP.c	FRRouting@@frr-frr-8.0.1-CVE-2024-31948-TP.c
Line	1318	1318
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-8.0.1-CVE-2024-31948-TP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1318.        for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1797
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-8.4.4-CVE-2023-46753-TP.c at line 1332 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-46753-TP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-46753-TP.c
Line	1342	1342
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-8.4.4-CVE-2023-46753-TP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1342.        for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1798
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-8.4.4-CVE-2023-47235-TP.c at line 1332 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2023-47235-TP.c	FRRouting@@frr-frr-8.4.4-CVE-2023-47235-TP.c
Line	1342	1342
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-8.4.4-CVE-2023-47235-TP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1342.        for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1799
Status	New

The buffer allocated by <= in FRRouting@@frr-frr-8.4.4-CVE-2024-31948-TP.c at line 1332 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	FRRouting@@frr-frr-8.4.4-CVE-2024-31948-TP.c	FRRouting@@frr-frr-8.4.4-CVE-2024-31948-TP.c
Line	1342	1342
Object	<=	<=

Code Snippet
File Name FRRouting@@frr-frr-8.4.4-CVE-2024-31948-TP.c
Method bgp_attr_flags_diagnose(struct bgp_attr_parser_args *args,

```
....
1342.        for (i = 0; i <= 2; i++) /* O,T,P, but not E */
```

Potential Off by One Error in Loops\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1800
Status	New

The buffer allocated by <= in glfw@@glfw-3.3.5-CVE-2021-3520-FP.c at line 604 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	glfw@@glfw-3.3.5-CVE-2021-3520-FP.c	glfw@@glfw-3.3.5-CVE-2021-3520-FP.c
Line	625	625
Object	<=	<=

Code Snippet
File Name glfw@@glfw-3.3.5-CVE-2021-3520-FP.c
Method static void draw_fountain(void)

```
....
625.                for (m = 0;  m <= FOUNTAIN_SWEEP_STEPS;  m++)
```

Use of Obsolete Functions

Query Path:
CPP\Cx\CPP Low Visibility\Use of Obsolete Functions Version:0

Categories

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

Description

Use of Obsolete Functions\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3276
Status	New

Method *mingw_fopen in git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c, at line 572, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	593	593
Object	_wfopen	_wfopen

Code Snippet
File Name git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
593.          file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 2:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3277
Status	New

Method *mingw_fopen in git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c, at line 585, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	606	606
Object	_wfopen	_wfopen

Code Snippet

File Name git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c

Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
606.        file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3278
Status	New

Method *mingw_fopen in git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c, at line 588, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	609	609
Object	_wfopen	_wfopen

Code Snippet

File Name git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c

Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
609.        file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15

	&pathid=3279
Status	New

Method *mingw_fopen in git@@git-v2.30.1-CVE-2021-21300-TP.c, at line 588, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	609	609
Object	_wfopen	_wfopen

Code Snippet
File Name git@@git-v2.30.1-CVE-2021-21300-TP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
609.         file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3280
Status	New

Method *mingw_fopen in git@@git-v2.30.3-CVE-2021-21300-FP.c, at line 591, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	612	612
Object	_wfopen	_wfopen

Code Snippet
File Name git@@git-v2.30.3-CVE-2021-21300-FP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
612.         file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3281
Status	New

Method *mingw_fopen in git@@git-v2.30.8-CVE-2021-21300-FP.c, at line 591, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c
Line	612	612
Object	_wfopen	_wfopen

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
612.         file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3282
Status	New

Method *mingw_fopen in git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c, at line 590, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	611	611
Object	_wfopen	_wfopen

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
611.         file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3283
Status	New

Method *mingw_fopen in git@@git-v2.33.0-CVE-2021-21300-FP.c, at line 611, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c

Line	632	632
Object	_wfopen	_wfopen

Code Snippet
File Name git@@git-v2.33.0-CVE-2021-21300-FP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
632.        file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3284
Status	New

Method *mingw_fopen in git@@git-v2.34.1-CVE-2021-21300-FP.c, at line 611, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	632	632
Object	_wfopen	_wfopen

Code Snippet
File Name git@@git-v2.34.1-CVE-2021-21300-FP.c
Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
632.        file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3285
Status	New

Method *mingw_fopen in git@@git-v2.37.0-CVE-2021-21300-FP.c, at line 614, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	635	635
Object	_wfopen	_wfopen

Code Snippet	
File Name	git@@git-v2.37.0-CVE-2021-21300-FP.c
Method	FILE *mingw_fopen (const char *filename, const char *otype)

```
....
635.         file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3286
Status	New

Method *mingw_fopen in git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c, at line 615, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Line	636	636
Object	_wfopen	_wfopen

Code Snippet	
File Name	git@@git-v2.38.0-rc2-CVE-2021-21300-FP.c
Method	FILE *mingw_fopen (const char *filename, const char *otype)

```
....
636.         file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3287
Status	New

Method *mingw_fopen in git@@git-v2.39.5-CVE-2021-21300-FP.c, at line 618, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.39.5-CVE-2021-21300-FP.c	git@@git-v2.39.5-CVE-2021-21300-FP.c
Line	639	639
Object	_wfopen	_wfopen

Code Snippet	
File Name	git@@git-v2.39.5-CVE-2021-21300-FP.c
Method	FILE *mingw_fopen (const char *filename, const char *otype)

```
....
639.         file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3288
Status	New

Method *mingw_fopen in git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c, at line 625, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c
Line	646	646
Object	_wfopen	_wfopen

Code Snippet

File Name git@@git-v2.41.0-rc0-CVE-2021-21300-FP.c

Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
646.         file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3289
Status	New

Method *mingw_fopen in git@@git-v2.42.0-CVE-2021-21300-FP.c, at line 625, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.42.0-CVE-2021-21300-FP.c	git@@git-v2.42.0-CVE-2021-21300-FP.c
Line	646	646
Object	_wfopen	_wfopen

Code Snippet

File Name git@@git-v2.42.0-CVE-2021-21300-FP.c

Method FILE *mingw_fopen (const char *filename, const char *otype)

```
....
646.         file = _wfopen(wfilename, wotype);
```

Use of Obsolete Functions\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3290
Status	New

Method *mingw_fopen in git@@git-v2.43.1-CVE-2021-21300-FP.c, at line 627, calls an obsolete API, _wfopen. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	git@@git-v2.43.1-CVE-2021-21300-FP.c	git@@git-v2.43.1-CVE-2021-21300-FP.c
Line	648	648
Object	_wfopen	_wfopen

Code Snippet

File Name	git@@git-v2.43.1-CVE-2021-21300-FP.c
Method	FILE *mingw_fopen (const char *filename, const char *otype)

```
....
648.         file = _wfopen(wfilename, wotype);
```

Insecure Temporary File

Query Path:

CPP\Cx\CPP Low Visibility\Insecure Temporary File Version:0

Categories

NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Insecure Temporary File\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1938
Status	New

	Source	Destination
File	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Line	994	994
Object	mktemp	mktemp

Code Snippet

File Name	git@@git-v2.26.0-rc1-CVE-2021-21300-TP.c
Method	int mkstemp(char *template)

```
....
994.         char *filename = mktemp(template);
```

Insecure Temporary File\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1939
Status	New

	Source	Destination
File	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Line	1016	1016
Object	mktemp	mktemp

Code Snippet

File Name	git@@git-v2.28.0-rc0-CVE-2021-21300-TP.c
Method	int mkstemp(char *template)

```
....
1016.        char *filename = mktemp(template);
```

Insecure Temporary File\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1940
Status	New

	Source	Destination
File	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Line	1019	1019
Object	mktemp	mktemp

Code Snippet

File Name	git@@git-v2.29.0-rc2-CVE-2021-21300-TP.c
Method	int mkstemp(char *template)

```
....
1019.        char *filename = mktemp(template);
```

Insecure Temporary File\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1941
Status	New

	Source	Destination
File	git@@git-v2.30.1-CVE-2021-21300-TP.c	git@@git-v2.30.1-CVE-2021-21300-TP.c
Line	1019	1019
Object	mktemp	mktemp

Code Snippet

File Name	git@@git-v2.30.1-CVE-2021-21300-TP.c
Method	int mkstemp(char *template)

```
....
1019.        char *filename = mktemp(template);
```

Insecure Temporary File\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1942
Status	New

	Source	Destination
File	git@@git-v2.30.3-CVE-2021-21300-FP.c	git@@git-v2.30.3-CVE-2021-21300-FP.c
Line	1022	1022
Object	mktemp	mktemp

Code Snippet

File Name	git@@git-v2.30.3-CVE-2021-21300-FP.c
Method	int mkstemp(char *template)

```
....
1022.        char *filename = mktemp(template);
```

Insecure Temporary File\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1943
Status	New

	Source	Destination
File	git@@git-v2.30.8-CVE-2021-21300-FP.c	git@@git-v2.30.8-CVE-2021-21300-FP.c

Line	1022	1022
Object	mktemp	mktemp

Code Snippet
File Name git@@git-v2.30.8-CVE-2021-21300-FP.c
Method int mkstemp(char *template)

```
....
1022.         char *filename = mktemp(template);
```

Insecure Temporary File\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1944
Status	New

	Source	Destination
File	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c	git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Line	1023	1023
Object	mktemp	mktemp

Code Snippet
File Name git@@git-v2.32.0-rc0-CVE-2021-21300-FP.c
Method int mkstemp(char *template)

```
....
1023.         char *filename = mktemp(template);
```

Insecure Temporary File\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1945
Status	New

	Source	Destination
File	git@@git-v2.33.0-CVE-2021-21300-FP.c	git@@git-v2.33.0-CVE-2021-21300-FP.c
Line	1044	1044
Object	mktemp	mktemp

Code Snippet
File Name git@@git-v2.33.0-CVE-2021-21300-FP.c
Method int mkstemp(char *template)

```
....
1044.        char *filename = mktemp(template);
```

Insecure Temporary File\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1946
Status	New

	Source	Destination
File	git@@git-v2.34.1-CVE-2021-21300-FP.c	git@@git-v2.34.1-CVE-2021-21300-FP.c
Line	1044	1044
Object	mktemp	mktemp

Code Snippet

File Name	git@@git-v2.34.1-CVE-2021-21300-FP.c
Method	int mkstemp(char *template)

```
....
1044.        char *filename = mktemp(template);
```

Insecure Temporary File\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1947
Status	New

	Source	Destination
File	git@@git-v2.37.0-CVE-2021-21300-FP.c	git@@git-v2.37.0-CVE-2021-21300-FP.c
Line	1062	1062
Object	mktemp	mktemp

Code Snippet

File Name	git@@git-v2.37.0-CVE-2021-21300-FP.c
Method	int mkstemp(char *template)

```
....
1062.        char *filename = mktemp(template);
```

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=1000020&projectid=15&pathid=2686
Status	New

Method gguf_ex_write at line 23 of ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.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	ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.c	ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.c
Line	58	58
Object	rand	rand

Code Snippet
File Name ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.c
Method static bool gguf_ex_write(const std::string & fname) {

```
....
58.          int32_t n_dims = rand() % GGML_MAX_DIMS + 1;
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2687
Status	New

Method gguf_ex_write at line 23 of ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.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	ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.c	ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.c
Line	61	61
Object	rand	rand

Code Snippet
File Name ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.c

Method	static bool gguf_ex_write(const std::string & fname) {

```
....
61.             ne[j] = rand() % 10 + 1;
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2688
Status	New

Method main at line 76 of glfw@@glfw-3.3.1-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	glfw@@glfw-3.3.1-CVE-2021-3520-FP.c	glfw@@glfw-3.3.1-CVE-2021-3520-FP.c
Line	124	124
Object	rand	rand

Code Snippet

File Name	glfw@@glfw-3.3.1-CVE-2021-3520-FP.c
Method	int main(int argc, char** argv)

```
....
124.                    pixels[y * 16 + x] = rand() % 256;
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2689
Status	New

Method main at line 76 of glfw@@glfw-3.3.3-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	glfw@@glfw-3.3.3-CVE-2021-3520-FP.c	glfw@@glfw-3.3.3-CVE-2021-3520-FP.c
Line	124	124
Object	rand	rand

Code Snippet

File Name	glfw@@glfw-3.3.3-CVE-2021-3520-FP.c
Method	int main(int argc, char** argv)

```
....
124.                  pixels[y * 16 + x] = rand() % 256;
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2690
Status	New

Method init_particle at line 244 of glfw@@glfw-3.3.5-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	glfw@@glfw-3.3.5-CVE-2021-3520-FP.c	glfw@@glfw-3.3.5-CVE-2021-3520-FP.c
Line	254	254
Object	rand	rand

Code Snippet
File Name glfw@@glfw-3.3.5-CVE-2021-3520-FP.c
Method static void init_particle(PARTICLE *p, double t)

```
....
254.        p->vz = 0.7f + (0.3f / 4096.f) * (float) (rand() & 4095);
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2691
Status	New

Method init_particle at line 244 of glfw@@glfw-3.3.5-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	glfw@@glfw-3.3.5-CVE-2021-3520-FP.c	glfw@@glfw-3.3.5-CVE-2021-3520-FP.c
Line	257	257
Object	rand	rand

Code Snippet
File Name glfw@@glfw-3.3.5-CVE-2021-3520-FP.c
Method static void init_particle(PARTICLE *p, double t)

```
....
257.        xy_angle = (2.f * (float) M_PI / 4096.f) * (float) (rand() &
4095);
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2692
Status	New

Method main at line 76 of glfw@@glfw-3.3.7-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	glfw@@glfw-3.3.7-CVE-2021-3520-FP.c	glfw@@glfw-3.3.7-CVE-2021-3520-FP.c
Line	124	124
Object	rand	rand

Code Snippet
File Name glfw@@glfw-3.3.7-CVE-2021-3520-FP.c
Method int main(int argc, char** argv)

```
....
124.                    pixels[y * 16 + x] = rand() % 256;
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2693
Status	New

Method main at line 76 of glfw@@glfw-3.3.1-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	glfw@@glfw-3.3.1-CVE-2021-3520-FP.c	glfw@@glfw-3.3.1-CVE-2021-3520-FP.c
Line	119	119
Object	srand	srand

Code Snippet
File Name glfw@@glfw-3.3.1-CVE-2021-3520-FP.c
Method int main(int argc, char** argv)

```
....
119.          srand((unsigned int) glfwGetTimerValue());
```

Use of Insufficiently Random Values\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2694
Status	New

Method main at line 76 of glfw@@glfw-3.3.3-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	glfw@@glfw-3.3.3-CVE-2021-3520-FP.c	glfw@@glfw-3.3.3-CVE-2021-3520-FP.c
Line	119	119
Object	srand	srand

Code Snippet
File Name glfw@@glfw-3.3.3-CVE-2021-3520-FP.c
Method int main(int argc, char** argv)

```
....
119.          srand((unsigned int) glfwGetTimerValue());
```

Use of Insufficiently Random Values\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2695
Status	New

Method main at line 76 of glfw@@glfw-3.3.7-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	glfw@@glfw-3.3.7-CVE-2021-3520-FP.c	glfw@@glfw-3.3.7-CVE-2021-3520-FP.c
Line	119	119
Object	srand	srand

Code Snippet
File Name glfw@@glfw-3.3.7-CVE-2021-3520-FP.c
Method int main(int argc, char** argv)

```
....
119.         srand((unsigned int) glfwGetTimerValue());
```

Inconsistent Implementations

Query Path:

CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1766
Status	New

	Source	Destination
File	glfw@@glfw-3.3.5-CVE-2021-3520-FP.c	glfw@@glfw-3.3.5-CVE-2021-3520-FP.c
Line	955	955
Object	getopt	getopt

Code Snippet

File Name	glfw@@glfw-3.3.5-CVE-2021-3520-FP.c
Method	int main(int argc, char** argv)

```
....
955.     while ((ch = getopt(argc, argv, "fh")) != -1)
```

Inconsistent Implementations\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1767
Status	New

	Source	Destination
File	fribidi@@fribidi-v1.0.10-CVE-2022-25309-TP.c	fribidi@@fribidi-v1.0.10-CVE-2022-25309-TP.c
Line	265	265
Object	getopt_long	getopt_long

Code Snippet

File Name	fribidi@@fribidi-v1.0.10-CVE-2022-25309-TP.c
Method	main (

```
....
265.         c = getopt_long (argc, argv, "hVn:", long_options, 
&option_index);
```

Inconsistent Implementations\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1768
Status	New

	Source	Destination
File	fribidi@@fribidi-v1.0.11-CVE-2022-25309-TP.c	fribidi@@fribidi-v1.0.11-CVE-2022-25309-TP.c
Line	265	265
Object	getopt_long	getopt_long

Code Snippet
File Name fribidi@@fribidi-v1.0.11-CVE-2022-25309-TP.c
Method main (

```
....
265.         c = getopt_long (argc, argv, "hVn:", long_options, 
&option_index);
```

Inconsistent Implementations\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1769
Status	New

	Source	Destination
File	fribidi@@fribidi-v1.0.12-CVE-2022-25309-FP.c	fribidi@@fribidi-v1.0.12-CVE-2022-25309-FP.c
Line	265	265
Object	getopt_long	getopt_long

Code Snippet
File Name fribidi@@fribidi-v1.0.12-CVE-2022-25309-FP.c
Method main (

```
....
265.         c = getopt_long (argc, argv, "hVn:", long_options, 
&option_index);
```

Inconsistent Implementations\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1770
Status	New

	Source	Destination
File	fribidi@@fribidi-v1.0.13-CVE-2022-25309-FP.c	fribidi@@fribidi-v1.0.13-CVE-2022-25309-FP.c
Line	265	265
Object	getopt_long	getopt_long

Code Snippet
File Name fribidi@@fribidi-v1.0.13-CVE-2022-25309-FP.c
Method main (

```
....
265.          c = getopt_long (argc, argv, "hVn:", long_options,
&option_index);
```

Inconsistent Implementations\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1771
Status	New

	Source	Destination
File	fribidi@@fribidi-v1.0.14-CVE-2022-25309-FP.c	fribidi@@fribidi-v1.0.14-CVE-2022-25309-FP.c
Line	265	265
Object	getopt_long	getopt_long

Code Snippet
File Name fribidi@@fribidi-v1.0.14-CVE-2022-25309-FP.c
Method main (

```
....
265.          c = getopt_long (argc, argv, "hVn:", long_options,
&option_index);
```

Inconsistent Implementations\Path 7:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1772
Status	New

	Source	Destination
File	fribidi@@fribidi-v1.0.9-CVE-2022-25309-TP.c	fribidi@@fribidi-v1.0.9-CVE-2022-25309-TP.c
Line	265	265
Object	getopt_long	getopt_long

Code Snippet
File Name fribidi@@fribidi-v1.0.9-CVE-2022-25309-TP.c
Method main (

```
....
265.          c = getopt_long (argc, argv, "hVn:", long_options,
&option_index);
```

Inconsistent Implementations\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1773
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	493	493
Object	getopt_long	getopt_long

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static void parse_options(int argc, char *const *argv)

```
....
493.                c = getopt_long(argc, argv,
```

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=1000020&projectid=15&pathid=1930
Status	New

The size of the buffer used by bgp_route_refresh_receive in "%s.%d.%d", at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to "%s.%d.%d", at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Line	1870	1870
Object	"%s.%d.%d"	"%s.%d.%d"

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2022-37032-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1870.                           sprintf(name, "%s.%d.%d", peer->host, afi,
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1931
Status	New

The size of the buffer used by bgp_route_refresh_receive in "%s.%d.%d", at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to "%s.%d.%d", at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Line	1870	1870
Object	"%s.%d.%d"	"%s.%d.%d"

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2023-47234-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1870.                           sprintf(name, "%s.%d.%d", peer->host, afi,
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1932
Status	New

The size of the buffer used by bgp_route_refresh_receive in "%s.%d.%d", at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to "%s.%d.%d", at line 1767 of FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Line	1870	1870
Object	"%s.%d.%d"	"%s.%d.%d"

Code Snippet
File Name FRRouting@@frr-frr-7.2.1-CVE-2024-31949-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1870.                          sprintf(name, "%s.%d.%d", peer->host, afi,
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1933
Status	New

The size of the buffer used by bgp_route_refresh_receive in "%s.%d.%d", at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to "%s.%d.%d", at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Line	1874	1874
Object	"%s.%d.%d"	"%s.%d.%d"

Code Snippet
File Name FRRouting@@frr-frr-7.3.1-CVE-2022-37032-TP.c
Method static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1874.                          sprintf(name, "%s.%d.%d", peer->host, afi,
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1934
Status	New

The size of the buffer used by bgp_route_refresh_receive in "%s.%d.%d", at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to "%s.%d.%d", at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Line	1874	1874
Object	"%s.%d.%d"	"%s.%d.%d"

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2023-47234-TP.c
Method	static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1874.                           sprintf(name, "%s.%d.%d", peer->host, afi,
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1935
Status	New

The size of the buffer used by bgp_route_refresh_receive in "%s.%d.%d", at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bgp_route_refresh_receive passes to "%s.%d.%d", at line 1769 of FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c, to overwrite the target buffer.

	Source	Destination
File	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Line	1874	1874
Object	"%s.%d.%d"	"%s.%d.%d"

Code Snippet

File Name	FRRouting@@frr-frr-7.3.1-CVE-2024-31949-TP.c
Method	static int bgp_route_refresh_receive(struct peer *peer, bgp_size_t size)

```
....
1874.                         sprintf(name, "%s.%d.%d", peer->host, afi,
```

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=1000020&projectid=15&pathid=2679
Status	New

The system data read by main in the file FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c at line 917 is potentially exposed by main found in FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c at line 917.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	928	967
Object	errno	printf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method int main(int argc, char **argv)

```
....
928.                fatal("stat %s: %s", execname, strerror(errno));
....
967.                     printf("%s already running.\n", execname);
```

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=1000020&projectid=15&pathid=2680
Status	New

The system data read by main in the file FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c at line 917 is potentially exposed by main found in FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c at line 917.

	Source	Destination

File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	1030	1029
Object	errno	printf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method int main(int argc, char **argv)

```
....
1030.                                 strerror(errno));
....
1029.                          printf("ioctl TIOCNOTTY failed: %s\n",
```

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=1000020&projectid=15&pathid=2681
Status	New

The system data read by main in the file FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c at line 917 is potentially exposed by main found in FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c at line 917.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	928	1029
Object	errno	printf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method int main(int argc, char **argv)

```
....
928.              fatal("stat %s: %s", execname, strerror(errno));
....
1029.                          printf("ioctl TIOCNOTTY failed: %s\n",
```

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=1000020&projectid=15&pathid=2682
Status	New

The system data read by do_stop in the file FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c at line 709 is potentially exposed by do_stop found in FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c at line 709.

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	733	732
Object	errno	printf

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static void do_stop(int signal_nr, int quietmode, int *n_killed,

```
....
733.                              progname, (long)p->pid, strerror(errno));
....
732.                      printf("%s: warning: failed to kill %ld: %s\n",
```

Information Exposure Through Comments

Query Path:
CPP\Cx\CPP Low Visibility\Information Exposure Through Comments Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)

Description

Information Exposure Through Comments\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2683
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Line	496	496
Object	password 'p	password 'p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.7-CVE-2023-22741-TP.c
Method * STUN password 'pwd'. The received content should be

```
....
496.    * STUN password 'pwd'. The received content should be
```

Information Exposure Through Comments\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2684
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Line	496	496
Object	password 'p	password 'p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.8-CVE-2023-22741-TP.c
Method * STUN password 'pwd'. The received content should be

```
....
496.    * STUN password 'pwd'. The received content should be
```

Information Exposure Through Comments\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=2685
Status	New

	Source	Destination
File	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c	freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Line	496	496
Object	password 'p	password 'p

Code Snippet
File Name freeswitch@@sofia-sip-v1.13.9-CVE-2023-22741-TP.c
Method * STUN password 'pwd'. The received content should be

```
....
496.    * STUN password 'pwd'. The received content should be
```

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=1000020&projectid=15&pathid=3440
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-24824-TP.c	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-24824-TP.c
Line	515	515
Object	sizeof	sizeof

Code Snippet

File Name	github@@cmark-gfm-0.29.0.gfm.1-CVE-2023-24824-TP.c
Method	static void process_footnotes(cmark_parser *parser) {

```
....
515.       qsort(map->sorted, map->size, sizeof(cmark_map_entry *),
sort_footnote_by_ix);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3441
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-24824-TP.c	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-24824-TP.c
Line	523	523
Object	sizeof	sizeof

Code Snippet

File Name	github@@cmark-gfm-0.29.0.gfm.3-CVE-2023-24824-TP.c
Method	static void process_footnotes(cmark_parser *parser) {

```
....
523.       qsort(map->sorted, map->size, sizeof(cmark_map_entry *),
sort_footnote_by_ix);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=3442
Status	New

	Source	Destination
File	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-24824-TP.c	github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-24824-TP.c

Line	523	523
Object	sizeof	sizeof

Code Snippet
File Name github@@cmark-gfm-0.29.0.gfm.5-CVE-2023-24824-TP.c
Method static void process_footnotes(cmark_parser *parser) {

```
....
523.        qsort(map->sorted, map->size, sizeof(cmark_map_entry *),
sort_footnote_by_ix);
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Arithmenic Operation On Boolean\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1936
Status	New

	Source	Destination
File	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c	FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Line	408	408
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name FRRouting@@frr-frr-7.5.1-CVE-2023-46752-TP.c
Method static void parse_schedule_item(const char *string, struct schedule_item *item)

```
....
408.        } else if ((after_hyph = string + (string[0] == '-'))
```

Arithmenic Operation On Boolean\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000020&projectid=15&pathid=1937
Status	New

	Source	Destination
File	ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.c	ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.c
Line	204	204
Object	<	<

Code Snippet
File Name ggerganov@@llama.cpp-gguf-v0.4.0-CVE-2024-41130-TP.c
Method static bool gguf_ex_read_1(const std::string & fname) {

```
....
204.                for (int j = 0; j < MIN(10, ggml_nelements(cur)); ++j)
{
```

Buffer Overflow boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
```

```
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

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 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

Command Injection

Risk

What might happen

An attacker could run arbitrary system-level OS commands on the application server host. Depending on the application’s OS permissions, these could include:

- File actions (read / create / modify / delete)
- Open a network connection to the attacker’s server
- Start and stop system services
- Modify the running application
- Complete server takeover

Cause

How does it happen

The application runs an OS system-level command to complete it's task, rather than via the application code. The command includes untrusted data, that may be controllable by an attacker. This untrusted string may contain malicious system-level commands engineered by an attacker, which could be executed as though the attacker were running commands directly on the application server.

In this case, the application receives data from the user input, and passes it as a string to the Operating System. This unvalidated data is then executed by the OS as a system command, running with the same system privileges as the application.

General Recommendations

How to avoid it

- Refactor the code to avoid any direct shell command execution. Instead, use platform provided APIs or library calls.
- If it is impossible to remove the command execution, execute only static commands that do not include dynamic, user-controlled data.
- Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified format, rather than rejecting bad patterns (blacklist). Parameters should be limited to an allowed character set, and non-validated input should be dropped. In addition to characters, check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
- In order to minimize damage as a measure of defense in depth, configure the application to run using a restricted user account that has no unnecessary OS privileges.
- If possible, isolate all OS commands to use a separate dedicated user account that has minimal privileges only for the specific commands and files used by the application, according to the Principle of Least Privilege.

- If absolutely necessary to call a system command or execute external program with user input, do not concatenate the user input with the command. Instead, isolate the parameters from the command by using a platform function that supports this.

- Do not call `system()` or it's variants, as this does not support separating data parameters from the system command.
- Instead, use one of the functions that receive arguments separately from the command, and validates them. This includes `ShellExecute()`, `execve()`, or one of it's variants.
- It is very important to pass user-controlled data to the function as the `lpParameters` or `argN` argument (or equivalent), and ensure that it is properly quoted. Never pass user controlled data to as the first parameter for `cmdname` or `filePath`.
- Do not directly execute any shell or command interpreters, such as `bash`, `cmd`, or `make`, with user-controlled input.

Source Code Examples

CPP

Execute System (Shell) Command With User Input

```
int main( int argc, char* argv[] )
{
      int result;
      if ( argc == 2 )
      {
             result = system(argv[1]);
      }
      return result;
}
```

Call External Program with Safe Parameters

```
int main( int argc, char* argv[] )
{
      int result;
      if ( argc == 2 )
      {
             char* param = escapeArg(argv[1]);

             result = _spawnl(_P_WAIT, EXTERNAL_PROGRAM_PATH, EXTERNAL_PROGRAM_PATH, param,
NULL);
      }
      return result;
}
```

Refactor Code to Use API Function

```
int main( int argc, char* argv[] )
{
      int result;
      if ( argc == 2 )
      {
            char* param = escapeArg(argv[1]);

            result = performSpecificAction(param);
      }
      return result;
}
```

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

Off by One Error in Methods

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

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;
}
```

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;
}
```

Improper Sanitization of Special Elements used in a Command ('Command Injection')

Weakness ID: 77 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not sanitize or incorrectly sanitizes special elements that could modify the intended command when it is sent to a downstream component.

Extended Description

Command injection vulnerabilities typically occur when:

1. Data enters the application from an untrusted source.

2. The data is part of a string that is executed as a command by the application.

3. By executing the command, the application gives an attacker a privilege or capability that the attacker would not otherwise have.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Access Control	Command injection allows for the execution of arbitrary commands and code by the attacker.
Integrity	If a malicious user injects a character (such as a semi-colon) that delimits the end of one command and the beginning of another, it may be possible to then insert an entirely new and unrelated command that was not intended to be executed.

Likelihood of Exploit

Very High

Demonstrative Examples

Example 1

The following simple program accepts a filename as a command line argument and displays the contents of the file back to the user. The program is installed setuid root because it is intended for use as a learning tool to allow system administrators in-training to inspect privileged system files without giving them the ability to modify them or damage the system.

Example Language: **C**

```
int main(char* argc, char** argv) {
char cmd[CMD_MAX] = "/usr/bin/cat ";
strcat(cmd, argv[1]);
system(cmd);
}
```

Because the program runs with root privileges, the call to system() also executes with root privileges. If a user specifies a standard filename, the call works as expected. However, if an attacker passes a string of the form ";rm -rf /", then the call to system() fails to execute cat due to a lack of arguments and then plows on to recursively delete the contents of the root partition.

Example 2

The following code is from an administrative web application designed to allow users to kick off a backup of an Oracle database using a batch-file wrapper around the rman utility and then run a cleanup.bat script to delete some temporary files. The script rmanDB.bat accepts a single command line parameter, which specifies what type of backup to perform. Because access to the database is restricted, the application runs the backup as a privileged user.

(Bad Code)

Example Language: **Java**

```
...
String btype = request.getParameter("backuptype");
String cmd = new String("cmd.exe /K \"
c:\\util\\rmanDB.bat "
+btype+
"&&c:\\utl\\cleanup.bat\"")
System.Runtime.getRuntime().exec(cmd);
...
```

The problem here is that the program does not do any validation on the backuptype parameter read from the user. Typically the Runtime.exec() function will not execute multiple commands, but in this case the program first runs the cmd.exe shell in order to run multiple commands with a single call to Runtime.exec(). Once the shell is invoked, it will happily execute multiple commands separated by two ampersands. If an attacker passes a string of the form "& del c:\\dbms\\*.*", then the application will execute this command along with the others specified by the program. Because of the nature of the application, it runs with the privileges necessary to interact with the database, which means whatever command the attacker injects will run with those privileges as well.

Example 3

The following code from a system utility uses the system property APPHOME to determine the directory in which it is installed and then executes an initialization script based on a relative path from the specified directory.

(Bad Code)

Example Language: **Java**

```
...
String home = System.getProperty("APPHOME");
String cmd = home + INITCMD;
java.lang.Runtime.getRuntime().exec(cmd);
...
```

The code above allows an attacker to execute arbitrary commands with the elevated privilege of the application by modifying the system property APPHOME to point to a different path containing a malicious version of INITCMD. Because the program does not validate the value read from the environment, if an attacker can control the value of the system property APPHOME, then they can fool the application into running malicious code and take control of the system.

Example 4

The following code is from a web application that allows users access to an interface through which they can update their password on the system. Part of the process for updating passwords in certain network environments is to run a make command in the /var/yp directory, the code for which is shown below.

(Bad Code)

Example Language: **Java**

```
...
System.Runtime.getRuntime().exec("make");
...
```

The problem here is that the program does not specify an absolute path for make and fails to clean its environment prior to executing the call to Runtime.exec(). If an attacker can modify the $PATH variable to point to a malicious binary called make and cause the program to be executed in their environment, then the malicious binary will be loaded instead of the one intended. Because of the nature of the application, it runs with the privileges necessary to perform system operations, which means the attacker's make will now be run with these privileges, possibly giving the attacker complete control of the system.

Example 5

The following code is a wrapper around the UNIX command cat which prints the contents of a file to standard out. It is also injectable:

(Bad Code)

Example Language: ***C***

```c
#include <stdio.h>
#include <unistd.h>

int main(int argc, char **argv) {

char cat[] = "cat ";
char *command;
size_t commandLength;

commandLength = strlen(cat) + strlen(argv[1]) + 1;
command = (char *) malloc(commandLength);
strncpy(command, cat, commandLength);
strncat(command, argv[1], (commandLength - strlen(cat)) );

system(command);
return (0);
}
```

Used normally, the output is simply the contents of the file requested:

```
$ ./catWrapper Story.txt
When last we left our heroes...
```

However, if we add a semicolon and another command to the end of this line, the command is executed by catWrapper with no complaint:

(Attack)

```
$ ./catWrapper Story.txt; ls
When last we left our heroes...
Story.txt
SensitiveFile.txt
PrivateData.db
a.out*
```

If catWrapper had been set to have a higher privilege level than the standard user, arbitrary commands could be executed with that higher privilege.

Potential Mitigations

Phase: Architecture and Design

If at all possible, use library calls rather than external processes to recreate the desired functionality

Phase: Implementation

If possible, ensure that all external commands called from the program are statically created.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

Run time: Run time policy enforcement may be used in a white-list fashion to prevent use of any non-sanctioned commands.

Assign permissions to the software system that prevents the user from accessing/opening privileged files.

Other Notes

Command injection is a common problem with wrapper programs.

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	Weakness Class	20	Improper Input Validation	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	74	Failure to Sanitize Data into a Different Plane ('Injection')	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	713	OWASP Top Ten 2007 Category A2 - Injection Flaws	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	Weaknesses in OWASP Top Ten (2004)711
ChildOf	Category	727	OWASP Top Ten 2004 Category A6 - Injection Flaws	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ParentOf	Weakness Base	78	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	88	Argument Injection or Modification	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	89	Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	90	Failure to Sanitize Data into LDAP Queries ('LDAP Injection')	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	624	Executable Regular Expression Error	**Development Concepts (primary)699** **Research Concepts (primary)1000**

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Command Injection
CLASP			Command injection

OWASP Top Ten 2007	A2	CWE More Specific	Injection Flaws
OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A6	CWE More Specific	Injection Flaws

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
15	Command Delimiters	
23	File System Function Injection, Content Based	
43	Exploiting Multiple Input Interpretation Layers	
75	Manipulating Writeable Configuration Files	
6	Argument Injection	
11	Cause Web Server Misclassification	
76	Manipulating Input to File System Calls	

References

G. Hoglund and G. McGraw. "Exploiting Software: How to Break Code". Addison-Wesley. February 2004.

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 Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Name		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Name		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Other Notes, Potential Mitigations		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Command Injection
2009-05-27	Failure to Sanitize Data into a Control Plane (aka 'Command Injection')
2009-07-27	Failure to Sanitize Data into a Control Plane ('Command Injection')

BACK TO TOP

Use of Hard coded Cryptographic Key

Risk

What might happen

Static, unchangeable encryption keys in the source code can be stolen by an attacker with access to the source code or the application binaries. Once the attacker has the encryption key, this can be used to gain access to any encrypted secret data, thus violating the confidentiality of the data. Furthermore, it would be impossible to replace the encryption key once stolen. Note that if this is a product that can be installed numerous times, the encryption key will always be the same, allowing an attacker to break all instances at the same cost.

Cause

How does it happen

The application code uses an encryption key to encrypt and decrypt sensitive data. While it is important to create this encryption key randomly and keep it secret, the application has a single, static key embedded in plain text in the source code.

An attacker could gain access to the source code - whether in the source control system, developer workstations, or the server filesystem or product binaries themselves. Once the attacker has gained access to the source code, it is trivial to retrieve the plain text encryption key and use it to decrypt the sensitive data that the application was protecting.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store any sensitive information, such as encryption keys, in plain text.
- Never hardcode encryption keys in the application source code.
- Implement proper key management, including dynamically generating random keys, protecting keys, and replacing keys as necessary.

Specific Recommendations:

- Remove the hardcoded encryption key from the application source code. Instead, retrieve the key from an external, protected store.

Source Code Examples

Java

Common example of hardcoded encryption key

```
//Generate a key
string encryptionKey = "EncryptionKey123"

//Encrypt the data
SecretKeySpec keySpec = new SecretKeySpec(encryptionKey.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
cipher.init(Cipher.ENCRYPT_MODE, keySpec);
output = cipher.doFinal(input)
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;

  void setPassword()
```

```
 {
      password = System.console().readLine("Enter your password: ");
  }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed
{
  private SealedObject password;
  void setPassword()
 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}

int main()
{
    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
      gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
      char* password = (char*) malloc(256);
      int i=0;
      char ch;
      ssize_t k;
      while(k = read(STDIN_FILENO, &ch, 1) > 0)
      {
            if (ch == '\n'){
                  password[i]='\0';
                  break;
            } else{
                  password[i++]=ch;
                  fflush(0);
            }
      }
      i=0;
      memset(password,'\0',256);
}

int main()

{

      printf("Please enter a password:\n");
      authfunc();
      somefunc();
      char ch;
      while(read(STDIN_FILENO, &ch, 1) > 0)
      {
            if (ch == '\n')
                  break;
      }
}
```

Use of Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Stored Buffer Overflow boundcpy

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
```

```
{

    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Inadequate Encryption Strength

Risk

What might happen

Using weak or outdated cryptography does not provide sufficient protection for sensitive data. An attacker that gains access to the encrypted data would likely be able to break the encryption, using either cryptanalysis or brute force attacks. Thus, the attacker would be able to steal user passwords and other personal data. This could lead to user impersonation or identity theft.

Cause

How does it happen

The application uses a weak algorithm, that is considered obselete since it is relatively easy to break. These obselete algorithms are vulnerable to several different kinds of attacks, including brute force.

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.
- Passwords should be protected with a dedicated password protection scheme, such as bcrypt, scrypt, PBKDF2, or Argon2.

Specific Recommendations:

- Do not use SHA-1, MD5, or any other weak hash algorithm to protect passwords or personal data. Instead, use a stronger hash such as SHA-256 when a secure hash is required.
- Do not use DES, Triple-DES, RC2, or any other weak encryption algorithm to protect passwords or personal data. Instead, use a stronger encryption algorithm such as AES to protect personal data.
- Do not use weak encryption modes such as ECB, or rely on insecure defaults. Explicitly specify a stronger encryption mode, such as GCM.
- For symmetric encryption, use a key length of at least 256 bits.

Source Code Examples

Java

Weakly Hashed PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.md5Hex(socialSecurityNum);
}
```

Stronger Hash for PII

```
string protectSSN(HttpServletRequest req) {
     string socialSecurityNum = req.getParameter("SocialSecurityNo");

     return DigestUtils.sha256Hex(socialSecurityNum);
}
```

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);
}
```

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 Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.

- Some implementations of the function carry significant security risks.

- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Inconsistent Implementations

BACK TO TOP

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
    - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
    - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

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

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699** **Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

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		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names	
Change Date	**Previous Entry Name**
2008-04-11	Code Quality

BACK TO TOP

Insecure Temporary File

Weakness ID: 377 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

Creating and using insecure temporary files can leave application and system data vulnerable to attack.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses a temporary file for storing intermediate data gathered from the network before it is processed.

(Bad Code)

Example Language: **C**

```
if (tmpnam_r(filename)) {

FILE* tmp = fopen(filename,"wb+");
while((recv(sock,recvbuf,DATA_SIZE, 0) > 0)&(amt!=0)) amt = fwrite(recvbuf,1,DATA_SIZE,tmp);
}
...
```

This otherwise unremarkable code is vulnerable to a number of different attacks because it relies on an insecure method for creating temporary files. The vulnerabilities introduced by this function and others are described in the following sections. The most egregious security problems related to temporary file creation have occurred on Unix-based operating systems, but Windows applications have parallel risks. This section includes a discussion of temporary file creation on both Unix and Windows systems. Methods and behaviors can vary between systems, but the fundamental risks introduced by each are reasonably constant.

Other Notes

Applications require temporary files so frequently that many different mechanisms exist for creating them in the C Library and Windows(R) API. Most of these functions are vulnerable to various forms of attacks.

The functions designed to aid in the creation of temporary files can be broken into two groups based whether they simply provide a filename or actually open a new file. - Group 1: "Unique" Filenames: The first group of C Library and WinAPI functions designed to help with the process of creating temporary files do so by generating a unique file name for a new temporary file, which the program is then supposed to open. This group includes C Library functions like tmpnam(), tempnam(), mktemp() and their C++ equivalents prefaced with an _ (underscore) as well as the GetTempFileName() function from the Windows API. This group of functions suffers from an underlying race condition on the filename chosen. Although the functions guarantee that the filename is unique at the time it is selected, there is no mechanism to prevent another process or an attacker from creating a file with the same name after it is selected but before the application attempts to open the file. Beyond the risk of a legitimate collision caused by another call to the same function, there is a high probability that an attacker will be able to create a malicious collision because the filenames generated by these functions are not sufficiently randomized to make them difficult to guess. If a file with the selected name is created, then depending on how the file is opened the existing contents or access permissions of the file may remain intact. If the existing contents of the file are malicious in nature, an attacker may be able to inject dangerous data into the application when it reads data back from the temporary file. If an attacker pre-creates the file with relaxed access permissions, then data stored in the temporary file by the application may be accessed, modified or corrupted by an attacker. On Unix based systems an even more insidious attack is possible if the attacker pre-creates the file as a link to another important file. Then, if the application truncates or writes data to the file, it may unwittingly perform damaging operations for the attacker. This is an especially serious threat if the program operates with elevated permissions. Finally, in the best case the file will be opened with the a call to open() using the O_CREAT and O_EXCL flags or to CreateFile() using the CREATE_NEW attribute, which will fail if the file already exists and therefore prevent the types of attacks described above. However, if an attacker is able to accurately predict a sequence of temporary file names, then the application may be prevented from opening necessary temporary storage causing a denial of service (DoS) attack. This type of attack would not be difficult to mount given the small amount of randomness used in the selection of the filenames generated by these functions. - Group 2: "Unique" Files: The second group of C Library functions attempts to resolve some of the security problems related to temporary files by not only generating a unique file name, but also opening the file. This group includes C Library functions like tmpfile() and its C++ equivalents prefaced with an _ (underscore), as well as the slightly better-behaved C Library function mkstemp(). The tmpfile() style functions construct a unique filename and open it in the same way that fopen() would if passed the flags "wb+", that is, as a binary file in read/write mode. If the file already exists, tmpfile() will truncate it to size zero, possibly in an attempt to assuage the security concerns mentioned earlier regarding the race condition that exists between the selection of a supposedly unique filename and the subsequent opening of the selected file. However, this behavior clearly does not solve the function's security problems. First, an attacker can pre-create the file with relaxed access-permissions that will likely be retained by the file opened by tmpfile(). Furthermore, on Unix based systems if the attacker pre-creates the file as a link to another important file, the application may use its possibly elevated permissions to truncate that file, thereby doing damage on behalf of the attacker. Finally, if tmpfile() does create a new file, the access permissions applied to that file will vary from one operating system to another, which can leave application data vulnerable even if an attacker is unable to predict the filename to be used in advance. Finally, mkstemp() is a reasonably safe way create temporary files. It will attempt to create and open a unique file based on a filename template provided by the user combined with a series of randomly generated characters. If it is unable to create such a file, it will fail and return -1. On modern systems the file is opened using mode 0600, which means the file will be secure from tampering unless the user explicitly changes its access permissions. However, mkstemp() still suffers from the use of predictable file names and can leave an application vulnerable to denial of service attacks if an attacker causes mkstemp() to fail by predicting and pre-creating the filenames to be used.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	376	Temporary File Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ParentOf	Weakness Base	378	Creation of Temporary File With Insecure Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	379	Creation of Temporary File in Directory with Incorrect Permissions	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Insecure Temporary File

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 23, "Creating Temporary Files Securely" Page 682. 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		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated References		

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**

```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 {
    //[..]
};
```

Information Leak Through Comments

Weakness ID: 615 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

Time of Introduction

- Implementation

Demonstrative Examples

Example 1

The following comment, embedded in a JSP, will be displayed in the resulting HTML output.

(Bad Code)

Example Languages: **HTML and JSP**

```
<!-- FIXME: calling this with more than 30 args kills the JDBC server -->
```

Observed Examples

Reference	Description
CVE-2007-6197	Version numbers and internal hostnames leaked in HTML comments.
CVE-2007-4072	CMS places full pathname of server in HTML comment.
CVE-2009-2431	blog software leaks real username in HTML comment.

Potential Mitigations

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Variant	540	Information Leak Through Source Code	**Development Concepts (primary)699** **Research Concepts (primary)1000**

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	Anonymous Tool Vendor (under NDA)		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal

	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Observed Examples, Taxonomy Mappings		

BACK TO TOP

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.
Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

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

Use of Obsolete Functions

Risk

What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions.
Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.

Cause

How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

General Recommendations

How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

Source Code Examples

Java

Using Deprecated Methods for Security Checks

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        secManager.checkMulticast(address, 0)
    }

}
```

A Replacement Security Check

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        SocketPermission permission = new SocketPermission(address.getHostAddress(),
"accept,connect");

        secManager.checkPermission(permission)
    }
```

```
  }
```

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--;
               }
            }
        }
```

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 Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-10-29	Unchecked Array Indexing

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025