

## vul\_files\_1\_1 Scan Report

Project Name	vul_files_1_1
Scan Start	Monday, January 6, 2025 4:06:28 PM
Preset	Checkmarx Default
Scan Time	02h:32m:01s
Lines Of Code Scanned	246298
Files Scanned	96
Report Creation Time	Monday, January 6, 2025 6:38:36 PM
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7</a>
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	5/1000 (Vulnerabilities/LOC)
Visibility	Public

## Filter Settings

### **Severity**

Included: High, Medium, Low, Information

Excluded: None

### **Result State**

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

Excluded: None

### **Assigned to**

Included: All

### **Categories**

Included:

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

Excluded:

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

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

**Results Limit**

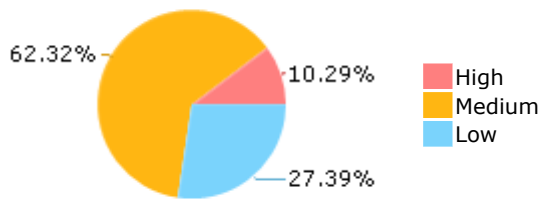
Results limit per query was set to 50

**Selected Queries**

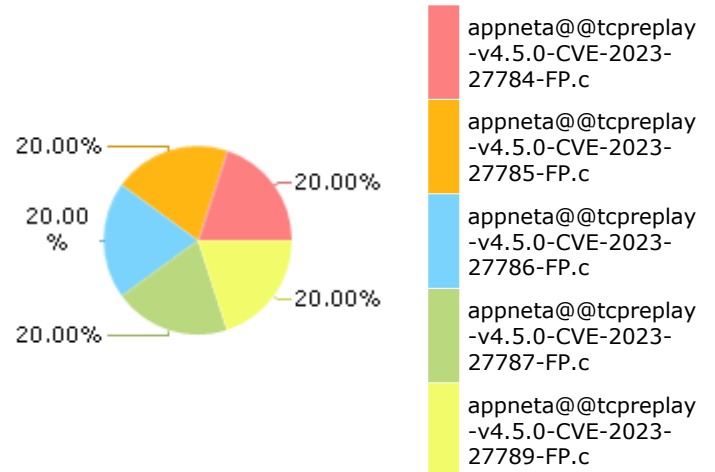
Selected queries are listed in [Result Summary](#)

---

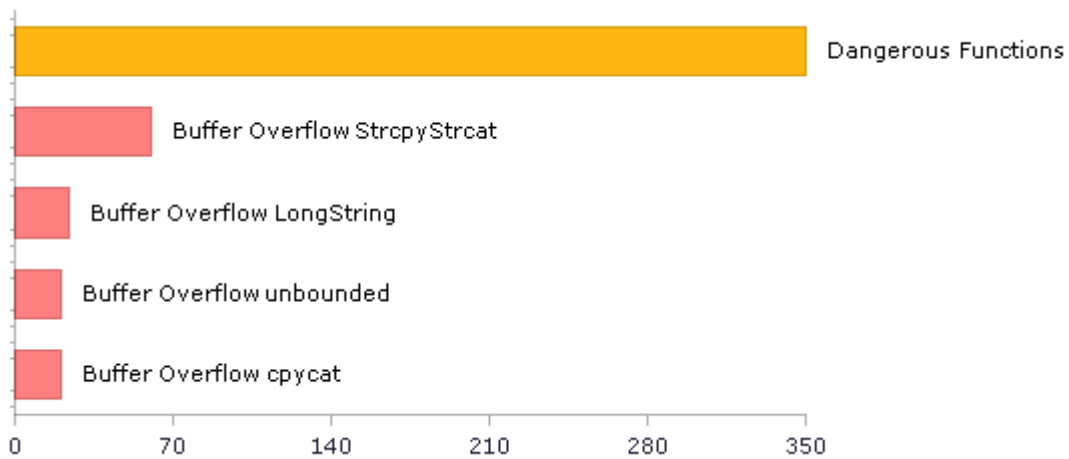
## Result Summary



## Most Vulnerable Files



## Top 5 Vulnerabilities



## Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: [OWASP Top 10 2017](https://owasp.org/Top10)

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	291	134
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	214	214
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
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	350	350
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

## Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: [OWASP Top 10 2013](#)

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	350	350
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	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	229	122
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.	9	9
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
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.	211	207
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.	0	0
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.	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 - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	214	214
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	6	2
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	336	143
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	124	17
SI-11 Error Handling (P2)*	38	38
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	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 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 wasn't 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

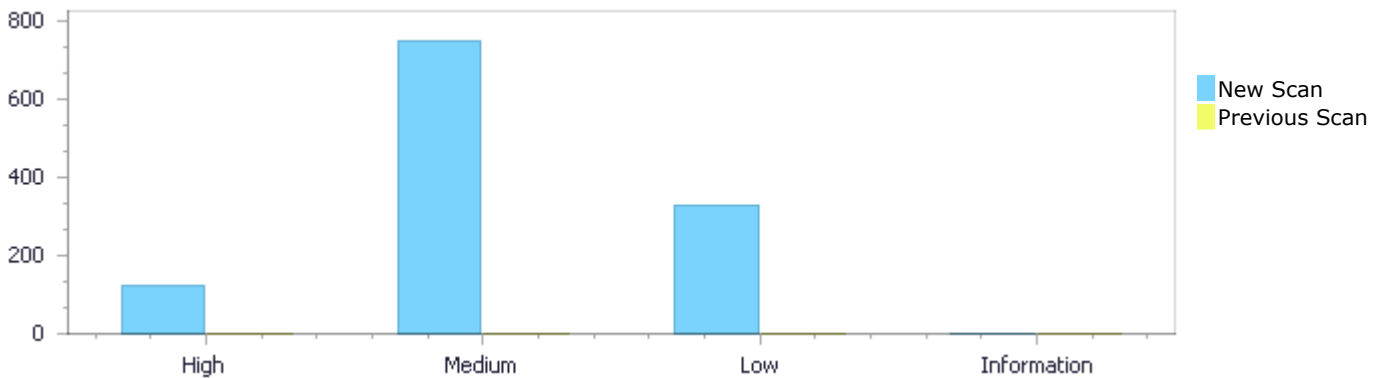
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

## Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	124	751	330	0	1,205
Recurrent Issues	0	0	0	0	0
Total	124	751	330	0	1,205

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	124	751	330	0	1,205
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	124	751	330	0	1,205

## Result Summary

Vulnerability Type	Occurrences	Severity
<a href="#">Buffer Overflow StrcpyStrcat</a>	60	High
<a href="#">Buffer Overflow LongString</a>	24	High
<a href="#">Buffer Overflow cpycat</a>	20	High
<a href="#">Buffer Overflow unbounded</a>	20	High
<a href="#">Dangerous Functions</a>	350	Medium

<a href="#">Use of Zero Initialized Pointer</a>	221	Medium
<a href="#">Buffer Overflow boundcpy WrongSizeParam</a>	105	Medium
<a href="#">Memory Leak</a>	50	Medium
<a href="#">Wrong Size t Allocation</a>	20	Medium
<a href="#">MemoryFree on StackVariable</a>	5	Medium
<a href="#">Improper Resource Access Authorization</a>	205	Low
<a href="#">NULL Pointer Dereference</a>	62	Low
<a href="#">Unchecked Return Value</a>	38	Low
<a href="#">Incorrect Permission Assignment For Critical Resources</a>	9	Low
<a href="#">TOCTOU</a>	7	Low
<a href="#">Reliance on DNS Lookups in a Decision</a>	6	Low
<a href="#">Unreleased Resource Leak</a>	3	Low

## 10 Most Vulnerable Files

### High and Medium Vulnerabilities

File Name	Issues Found
vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	31
vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	31
vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	31
vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	31
vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	31
vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c	18
vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c	18
vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c	18
vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c	18
vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c	18

# Scan Results Details

## Buffer Overflow StrcpyStrcat

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow StrcpyStrcat 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 StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=65">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=65</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	tempoctet

### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=66">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=66</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 3:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=67>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 4:

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

[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=68](http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=68)

Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c

Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 5:

Severity High

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=69>

Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c

Method cidr2cidr(char \*cidr)



```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=70">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=70</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=71">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=71</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c

Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 8:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=72>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 9:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=73>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 10:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=74>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 11:

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

[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=75](http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=75)

Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 12:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=76>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=77">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=77</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=78">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=78</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c

Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 15:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=79">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=79</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 16:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=80">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=80</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 17:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=81>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 18:

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

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=82">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=82</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 19:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=83">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=83</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)



```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow StrcpyStrcat\Path 20:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=84">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=84</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow StrcpyStrcat\Path 21:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=85">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=85</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c

Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 22:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=86>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 23:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=87>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 24:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=88">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=88</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 25:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=88">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=88</a>

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=89">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=89</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
204.         strcat(networkip, ".");
```

#### Buffer Overflow StrcpyStrcat\Path 26:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=90">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=90</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
204.                 strcat(networkip, ".");
```

### Buffer Overflow StrcpyStrcat\Path 27:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=91">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=91</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
204.                 strcat(networkip, ".");
```

### Buffer Overflow StrcpyStrcat\Path 28:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=92">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=92</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c

Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
204.         strcat(networkip, ".");
```

#### Buffer Overflow StrcpyStrcat\Path 29:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=93>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 30:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=94>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 31:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=95>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 32:

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

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=96">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=96</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 33:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=97">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=97</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)



```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
204.                 strcat(networkip, ".");
```

#### Buffer Overflow StrcpyStrcat\Path 34:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=98">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=98</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
204.                 strcat(networkip, ".");
```

#### Buffer Overflow StrcpyStrcat\Path 35:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=99">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=99</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c

Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
204.                                     strcat(networkip, ".");
```

#### Buffer Overflow StrcpyStrcat\Path 36:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=100>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
204.                                     strcat(networkip, ".");
```

#### Buffer Overflow StrcpyStrcat\Path 37:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=101>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 38:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=102>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 39:

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

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=103">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=103</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 40:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=104">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=104</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```

....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);

```

### Buffer Overflow StrcpyStrcat\Path 41:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=105">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=105</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	204
Object	Address	networkip

### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```

....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
204.         strcat(networkip, ".");

```

### Buffer Overflow StrcpyStrcat\Path 42:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=106">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=106</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c

Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
204.                                     strcat(networkip, ".");
```

#### Buffer Overflow StrcpyStrcat\Path 43:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=107>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
204.                                     strcat(networkip, ".");
```

#### Buffer Overflow StrcpyStrcat\Path 44:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=108>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
204.         strcat(networkip, ".");
```

#### Buffer Overflow StrcpyStrcat\Path 45:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=109>  
Status New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 46:

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

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=110">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=110</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 47:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=111">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=111</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)



```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 48:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=112">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=112</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow StrcpyStrcat\Path 49:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=113">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=113</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c

Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
204.                                     strcat(networkip, ".");
```

#### Buffer Overflow StrcpyStrcat\Path 50:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=114">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=114</a>
Status	New

The size of the buffer used by cidr2cidr in networkip, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	204
Object	Address	networkip

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
204.                                     strcat(networkip, ".");
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to `"127.0.0.1"`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	692	737
Object	<code>"127.0.0.1"</code>	<code>ip</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`  
Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....  
692.     name = "127.0.0.1";  
....  
737.     if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=  
4)
```

### Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=2">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=2</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to `"127.0.0.1"`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	692	745
Object	<code>"127.0.0.1"</code>	<code>ip</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`  
Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....
692.         name = "127.0.0.1";
....
745.                                     (unsigned)ip[3]));
```

### Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=3">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=3</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to "127.0.0.1", at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	692	743
Object	"127.0.0.1"	<code>ip</code>

### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`  
 Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....
692.         name = "127.0.0.1";
....
743.         cg->ip_addr = htonl((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

### Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=4">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=4</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to "127.0.0.1", at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	692	743

Object	"127.0.0.1"	ip
--------	-------------	----

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c  
Method httpGetHostByName(const char \*name) /\* I - Hostname or IP address \*/

```
....  
692.      name = "127.0.0.1";  
....  
743.      cg->ip_addr = htonl((((((unsigned)ip[0] << 8) |  
(unsigned)ip[1]) << 8) |
```

#### Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=5">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=5</a>
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	740
Object	"127.0.0.1"	ip

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c  
Method httpGetHostByName(const char \*name) /\* I - Hostname or IP address \*/

```
....  
692.      name = "127.0.0.1";  
....  
740.      if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

#### Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=6">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=6</a>
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	740
Object	"127.0.0.1"	ip

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c  
Method httpGetHostByName(const char \*name) /\* I - Hostname or IP address \*/

```
....  
692.     name = "127.0.0.1";  
....  
740.     if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

#### Buffer Overflow LongString\Path 7:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=7>  
Status New

The size of the buffer used by httpGetHostByName in ip, at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	692	740
Object	"127.0.0.1"	ip

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c  
Method httpGetHostByName(const char \*name) /\* I - Hostname or IP address \*/

```
....  
692.     name = "127.0.0.1";  
....  
740.     if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

#### Buffer Overflow LongString\Path 8:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=8>  
Status New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to `"127.0.0.1"`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	692	740
Object	<code>"127.0.0.1"</code>	<code>ip</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`

Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....
692.     name = "127.0.0.1";
....
740.     if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

#### Buffer Overflow LongString\Path 9:

Severity High

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=9>

Status New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to `"127.0.0.1"`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	692	737
Object	<code>"127.0.0.1"</code>	<code>ip</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`

Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....
692.     name = "127.0.0.1";
....
737.     if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)
```

#### Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=10">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=10</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to `"127.0.0.1"`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	692	737
Object	<code>"127.0.0.1"</code>	<code>ip</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`  
Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....  
692.     name = "127.0.0.1";  
....  
737.     if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=  
4)
```

#### Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=11">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=11</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to `"127.0.0.1"`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	692	737
Object	<code>"127.0.0.1"</code>	<code>ip</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`  
Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`



```

....
692.         name = "127.0.0.1";
....
737.         if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=
4)

```

### Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=12">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=12</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to "127.0.0.1", at line 676 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	692	744
Object	"127.0.0.1"	<code>ip</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`  
Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```

....
692.         name = "127.0.0.1";
....
744.                                     (unsigned)ip[2]) << 8) |

```

### Buffer Overflow LongString\Path 13:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=13">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=13</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to "127.0.0.1", at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>
Line	692	743

Object	"127.0.0.1"	ip
--------	-------------	----

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c  
 Method httpGetHostByName(const char \*name) /\* I - Hostname or IP address \*/

```
....
692.      name = "127.0.0.1";
....
743.      cg->ip_addr = htonl((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

#### Buffer Overflow LongString\Path 14:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=14">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=14</a>
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c
Line	692	743
Object	"127.0.0.1"	ip

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c  
 Method httpGetHostByName(const char \*name) /\* I - Hostname or IP address \*/

```
....
692.      name = "127.0.0.1";
....
743.      cg->ip_addr = htonl((((((unsigned)ip[0] << 8) |
(unsigned)ip[1]) << 8) |
```

#### Buffer Overflow LongString\Path 15:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=15">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=15</a>
Status	New

The size of the buffer used by httpGetHostByName in ip, at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that `httpGetHostByName` passes to "127.0.0.1", at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>
Line	692	740
Object	"127.0.0.1"	ip

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`  
Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....  
692.     name = "127.0.0.1";  
....  
740.     if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

#### Buffer Overflow LongString\Path 16:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=16>  
Status New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to "127.0.0.1", at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>
Line	692	740
Object	"127.0.0.1"	ip

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`  
Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....  
692.     name = "127.0.0.1";  
....  
740.     if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

#### Buffer Overflow LongString\Path 17:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=16>

Status [pathid=17](#)  
New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to `"127.0.0.1"`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>
Line	692	740
Object	<code>"127.0.0.1"</code>	<code>ip</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`

Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....  
692.     name = "127.0.0.1";  
....  
740.     if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

#### Buffer Overflow LongString\Path 18:

Severity High

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=18>

Status New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to `"127.0.0.1"`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>
Line	692	740
Object	<code>"127.0.0.1"</code>	<code>ip</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`

Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....  
692.     name = "127.0.0.1";  
....  
740.     if (ip[0] > 255 || ip[1] > 255 || ip[2] > 255 || ip[3] > 255)
```

**Buffer Overflow LongString\Path 19:**

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=19">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=19</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to `"127.0.0.1"`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>
Line	692	737
Object	<code>"127.0.0.1"</code>	<code>ip</code>

**Code Snippet**

File Name `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`  
Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....  
692.     name = "127.0.0.1";  
....  
737.     if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=  
4)
```

**Buffer Overflow LongString\Path 20:**

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=20">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=20</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to `"127.0.0.1"`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>
Line	692	737
Object	<code>"127.0.0.1"</code>	<code>ip</code>

**Code Snippet**

File Name `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`  
Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....  
692.      name = "127.0.0.1";  
....  
737.      if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=  
4)
```

### Buffer Overflow LongString\Path 21:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=21">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=21</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to "127.0.0.1", at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>
Line	692	737
Object	"127.0.0.1"	<code>ip</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`  
Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```
....  
692.      name = "127.0.0.1";  
....  
737.      if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=  
4)
```

### Buffer Overflow LongString\Path 22:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=22">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=22</a>
Status	New

The size of the buffer used by `httpGetHostByName` in `ip`, at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `httpGetHostByName` passes to "127.0.0.1", at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>

Line	692	737
Object	"127.0.0.1"	ip

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c  
Method httpGetHostByName(const char \*name) /\* I - Hostname or IP address \*/

```
....  
692.      name = "127.0.0.1";  
....  
737.      if (sscanf(name, "%u.%u.%u.%u", ip, ip + 1, ip + 2, ip + 3) !=  
4)
```

#### Buffer Overflow LongString\Path 23:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=23>  
Status New

The size of the buffer used by httpGetHostByName in ip, at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that httpGetHostByName passes to "127.0.0.1", at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c
Line	692	744
Object	"127.0.0.1"	ip

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c  
Method httpGetHostByName(const char \*name) /\* I - Hostname or IP address \*/

```
....  
692.      name = "127.0.0.1";  
....  
744.      (unsigned)ip[2]) << 8) |
```

#### Buffer Overflow LongString\Path 24:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=24>  
Status New

The size of the buffer used by httpGetHostByName in ip, at line 676 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that `httpGetHostByName` passes to "127.0.0.1", at line 676 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>
Line	692	745
Object	"127.0.0.1"	ip

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`  
 Method `httpGetHostByName(const char *name) /* I - Hostname or IP address */`

```

.....
692.         name = "127.0.0.1";
.....
745.                                     (unsigned)ip[3]));

```

## Buffer Overflow cpycat

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow cpycat Version:0

### 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 cpycat\Path 1:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=25">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=25</a>
Status	New

The size of the buffer used by `cidr2cidr` in `tempoctet`, at line 132 of `vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `cidr2cidr` passes to `Address`, at line 132 of `vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c`, to overwrite the target buffer.

	Source	Destination
File	<code>vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c</code>	<code>vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c</code>
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c`  
 Method `cidr2cidr(char *cidr)`



```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow cpycat\Path 2:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=26">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=26</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow cpycat\Path 3:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=27">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=27</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c

Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 4:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=28>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 5:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=29>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 6:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=30>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 7:

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

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=31">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=31</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 8:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=32">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=32</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow cpycat\Path 9:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=33">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=33</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow cpycat\Path 10:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=34">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=34</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c

Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 11:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=35">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=35</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 12:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=36">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=36</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 13:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=37>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 14:

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

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=38">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=38</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 15:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=39">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=39</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)



```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow cpycat\Path 16:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=40">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=40</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow cpycat\Path 17:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=41">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=41</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c

Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 18:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=42>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 19:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=43>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow cpycat\Path 20:

Severity High  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=44>  
Status New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

## Buffer Overflow unbounded

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow unbounded 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 unbounded\Path 1:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=45">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=45</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.     count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.     strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 2:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=46">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=46</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201

Object	Address	tempoctet
--------	---------	-----------

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 3:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=47">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=47</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 4:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=48">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=48</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 5:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=49">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=49</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 6:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=49">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=49</a>

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=50">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=50</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 7:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=51">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=51</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow unbounded\Path 8:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=52">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=52</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow unbounded\Path 9:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=53">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=53</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c



Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 10:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=54">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=54</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 11:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=55">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=55</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 12:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=56">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=56</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 13:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=56">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=56</a>

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=57">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=57</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 14:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=58">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=58</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow unbounded\Path 15:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=59">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=59</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

### Buffer Overflow unbounded\Path 16:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=60">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=60</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c

Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 17:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=61">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=61</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 18:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=62">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=62</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 19:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=63">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=63</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],  
    &octets[2], &octets[3], &newcidr->masklen);  
....  
201.         strcat(networkip, tempoctet);
```

#### Buffer Overflow unbounded\Path 20:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=63">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=63</a>

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=64">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=64</a>
Status	New

The size of the buffer used by cidr2cidr in tempoctet, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cidr2cidr passes to Address, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	158	201
Object	Address	tempoctet

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....
158.         count = sscanf(cidr, "%u.%u.%u.%u/%d", &octets[0], &octets[1],
&octets[2], &octets[3], &newcidr->masklen);
....
201.         strcat(networkip, tempoctet);
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=250">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=250</a>
Status	New

The dangerous function, alloca, was found in use at line 231 in vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	231	231
Object	alloca	alloca

**Code Snippet**

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
231.      path      = alloca(path_len);
```

**Dangerous Functions\Path 2:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=251>  
Status New

The dangerous function, `alloca`, was found in use at line 215 in `vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c` file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	231	231
Object	alloca	alloca

**Code Snippet**

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
231.      path      = alloca(path_len);
```

**Dangerous Functions\Path 3:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=252>  
Status New

The dangerous function, `alloca`, was found in use at line 215 in `vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c` file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	231	231
Object	alloca	alloca



**Code Snippet**

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
231.      path      = alloca(path_len);
```

**Dangerous Functions\Path 4:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=253>  
Status New

The dangerous function, `alloca`, was found in use at line 213 in `vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c` file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	229	229
Object	alloca	alloca

**Code Snippet**

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
229.      path      = alloca(path_len);
```

**Dangerous Functions\Path 5:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=254>  
Status New

The dangerous function, `alloca`, was found in use at line 213 in `vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c` file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	229	229

Object	alloca	alloca
--------	--------	--------

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
229.      path      = alloca(path_len);
```

#### Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=255">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=255</a>
Status	New

The dangerous function, `alloca`, was found in use at line 201 in `vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c` file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	217	217
Object	alloca	alloca

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
217.      path      = alloca(path_len);
```

#### Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=256">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=256</a>
Status	New

The dangerous function, `alloca`, was found in use at line 201 in `vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c` file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c

Line	217	217
Object	alloca	alloca

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
217.      path      = alloca(path_len);
```

#### Dangerous Functions\Path 8:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=257>

Status New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27784-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	100	100
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27784-TP.c

Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....
100.      memcpy(newstr, str, strlen(str) + 1);
```

#### Dangerous Functions\Path 9:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=258>

Status New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27784-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

Source	Destination
--------	-------------

File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	313	313
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=259">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=259</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=260">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=260</a>
Status	New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	100	100
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c

Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.      memcpy(newstr, str, strlen(str) + 1);
```

#### Dangerous Functions\Path 12:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=261>

Status New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	313	313
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c

Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 13:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=262>

Status New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.          memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=263">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=263</a>
Status	New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	100	100
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.          memcpy(newstr, str, strlen(str) + 1);
```

#### Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=264">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=264</a>

Status New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	313	313
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c

Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 16:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=265>

Status New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c

Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 17:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=265>

Status [pathid=266](#)  
New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	100	100
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.      memcpy(newstr, str, strlen(str) + 1);
```

#### Dangerous Functions\Path 18:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=267>  
Status New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	313	313
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 19:

Severity Medium  
Result State To Verify



Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=268">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=268</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.         memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=269">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=269</a>
Status	New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	100	100
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.         memcpy(newstr, str, strlen(str) + 1);
```

#### Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=270">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=270</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27789-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	313	313
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27789-TP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=271">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=271</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27789-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27789-TP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.      memcpy(&hex[numbytes], &databyte, 1);
```

**Dangerous Functions\Path 23:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=272">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=272</a>
Status	New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c
Line	100	100
Object	memcpy	memcpy

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.      memcpy(newstr, str, strlen(str) + 1);
```

**Dangerous Functions\Path 24:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=273">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=273</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c
Line	313	313
Object	memcpy	memcpy

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

### Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=274">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=274</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.      memcpy(&hex[numbytes], &databyte, 1);
```

### Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=275">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=275</a>
Status	New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c
Line	100	100
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c

Method `_our_safe_strdup(const char *str, const char *funcname, const int line, const char *file)`

```
....  
100.      memcpy(newstr, str, strlen(str) + 1);
```

### Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=276">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=276</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c
Line	313	313
Object	memcpy	memcpy

### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c`  
Method `read_hexstring(const char *l2string, u_char *hex, const int hexlen)`

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

### Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=277">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=277</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c
Line	326	326
Object	memcpy	memcpy

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c

Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.          memcpy(&hex[numbytes], &databyte, 1);
```

**Dangerous Functions\Path 29:**

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=278>

Status New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c
Line	100	100
Object	memcpy	memcpy

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c

Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.          memcpy(newstr, str, strlen(str) + 1);
```

**Dangerous Functions\Path 30:**

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=279>

Status New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c
Line	313	313

Object	memcpy	memcpy
--------	--------	--------

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcp replay-v4.3.4-beta1-CVE-2023-27786-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=280">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=280</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcp replay-v4.3.4-beta1-CVE-2023-27786-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcp replay-v4.3.4-beta1-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcp replay-v4.3.4-beta1-CVE-2023-27786-FP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcp replay-v4.3.4-beta1-CVE-2023-27786-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=281">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=281</a>
Status	New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcp replay-v4.3.4-beta1-CVE-2023-27787-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcp replay-v4.3.4-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcp replay-v4.3.4-beta1-CVE-2023-27787-FP.c

Line	100	100
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c

Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.      memcpy(newstr, str, strlen(str) + 1);
```

#### Dangerous Functions\Path 33:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=282>

Status New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c
Line	313	313
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c

Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 34:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=283>

Status New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

Source	Destination
--------	-------------



File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=284">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=284</a>
Status	New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c
Line	100	100
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.      memcpy(newstr, str, strlen(str) + 1);
```

#### Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=285">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=285</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c
Line	313	313
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=286">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=286</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=287">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=287</a>
Status	New

The dangerous function, memcpy, was found in use at line 205 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c
Line	238	238
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c  
Method dlt\_jnpr\_ether\_decode(tcpeditdlt\_t \*ctx, const u\_char \*packet, const int pktlen)

```
....  
238.      memcpy(&jnpr_header_len, &packet[JUNIPER_ETHER_EXTLEN_OFFSET],  
2);
```

#### Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=288">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=288</a>
Status	New

The dangerous function, memcpy, was found in use at line 290 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c
Line	315	315
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c  
Method dlt\_jnpr\_ether\_proto(tcpeditdlt\_t \*ctx, const u\_char \*packet, const int pktlen)

```
....  
315.      memcpy(&jnpr_hdr_len, &packet[JUNIPER_ETHER_EXTLEN_OFFSET],  
2);
```

#### Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=289">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=289</a>
Status	New

The dangerous function, memcpy, was found in use at line 379 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c
Line	394	394
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c  
Method dlt\_jnpr\_ether\_get\_mac(tcpeditdlt\_t \*ctx, tcpeditdlt\_mac\_type\_t mac, const u\_char \*packet, const int pktlen)

```
....  
394.      memcpy(&jnpr_hdr_len, &packet[JUNIPER_ETHER_EXTLEN_OFFSET],  
2);
```

#### Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=290">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=290</a>
Status	New

The dangerous function, memcpy, was found in use at line 407 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c
Line	421	421
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27783-TP.c  
Method dlt\_jnpr\_ether\_l2len(tcpeditdlt\_t \*ctx, const u\_char \*packet, const int pktlen)

```
....  
421.      memcpy(&len, &packet[JUNIPER_ETHER_EXTLEN_OFFSET], 2);
```

#### Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=290">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=290</a>

Status [pathid=291](#)  
New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c
Line	100	100
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.      memcpy(newstr, str, strlen(str) + 1);
```

#### Dangerous Functions\Path 43:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=292>  
Status New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c
Line	313	313
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 44:

Severity Medium  
Result State To Verify

Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=293">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=293</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.         memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=294">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=294</a>
Status	New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c
Line	100	100
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.         memcpy(newstr, str, strlen(str) + 1);
```

#### Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=295">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=295</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c
Line	313	313
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
313.      memcpy(&hex[numbytes], &databyte, 1);
```

#### Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=296">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=296</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c
Line	326	326
Object	memcpy	memcpy

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....  
326.      memcpy(&hex[numbytes], &databyte, 1);
```

**Dangerous Functions\Path 48:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=297">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=297</a>
Status	New

The dangerous function, memcpy, was found in use at line 91 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c
Line	100	100
Object	memcpy	memcpy

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
100.      memcpy(newstr, str, strlen(str) + 1);
```

**Dangerous Functions\Path 49:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=298">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=298</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c
Line	313	313
Object	memcpy	memcpy

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)



```
....
313.      memcpy(&hex[numbytes], &databyte, 1);
```

### Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=299">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=299</a>
Status	New

The dangerous function, memcpy, was found in use at line 289 in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c
Line	326	326
Object	memcpy	memcpy

### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c  
Method read\_hexstring(const char \*l2string, u\_char \*hex, const int hexlen)

```
....
326.      memcpy(&hex[numbytes], &databyte, 1);
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=764">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=764</a>
Status	New

The variable declared in next at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 144 is not initialized when it is used by new\_list at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 161.

Source	Destination
--------	-------------

File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	156	167
Object	next	new_list

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method copy\_invalidate\_t(invalidate\_t \*i)

```
....
156.     iptr->next      = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method copy\_config(invalidate\_t \*old\_list)

```
....
167.     new_list = copy_invalidate_t(old_list);
```

#### Use of Zero Initialized Pointer\Path 2:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=765>  
Status New

The variable declared in next at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 144 is not initialized when it is used by new\_list at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 161.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	156	167
Object	next	new_list

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method copy\_invalidate\_t(invalidate\_t \*i)

```
....
156.     iptr->next      = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method copy\_config(invalidate\_t \*old\_list)

```
....
167.         new_list = copy_invalidate_t(old_list);
```

### Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=766">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=766</a>
Status	New

The variable declared in next at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 144 is not initialized when it is used by new\_list at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 161.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	156	167
Object	next	new_list

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method copy\_invalidate\_t(invalidate\_t \*i)

```
....
156.     iptr->next      = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method copy\_config(invalidate\_t \*old\_list)

```
....
167.         new_list = copy_invalidate_t(old_list);
```

### Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=767">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=767</a>
Status	New

The variable declared in next at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 142 is not initialized when it is used by new\_list at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 159.

Source	Destination
--------	-------------

File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	154	165
Object	next	new_list

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method copy\_invalidate\_t(invalidate\_t \*i)

```
....
154.      iptr->next      = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method copy\_config(invalidate\_t \*old\_list)

```
....
165.      new_list = copy_invalidate_t(old_list);
```

#### Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=768">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=768</a>
Status	New

The variable declared in next at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 142 is not initialized when it is used by new\_list at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 159.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	154	165
Object	next	new_list

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method copy\_invalidate\_t(invalidate\_t \*i)

```
....
154.      iptr->next      = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method copy\_config(invalidate\_t \*old\_list)

```
....
165.         new_list = copy_invalidate_t(old_list);
```

### Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=769">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=769</a>
Status	New

The variable declared in next at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 130 is not initialized when it is used by new\_list at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 147.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	142	153
Object	next	new_list

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method copy\_invalidate\_t(invalidate\_t \*i)

```
....
142.     iptr->next      = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method copy\_config(invalidate\_t \*old\_list)

```
....
153.         new_list = copy_invalidate_t(old_list);
```

### Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=770">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=770</a>
Status	New

The variable declared in next at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 130 is not initialized when it is used by new\_list at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 147.

Source	Destination
--------	-------------

File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	142	153
Object	next	new_list

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method copy\_invalidate\_t(invalidate\_t \*i)

```
....
142.      iptr->next      = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method copy\_config(invalidate\_t \*old\_list)

```
....
153.      new_list = copy_invalidate_t(old_list);
```

#### Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=771">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=771</a>
Status	New

The variable declared in token at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c in line 291 is not initialized when it is used by map at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c in line 328.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	295	328
Object	token	map

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method parse\_endpoints(tcpr\_cidrmap\_t \*\*cidrmap1, tcpr\_cidrmap\_t \*\*cidrmap2, const char \*optarg)

```
....
295.      char *token = NULL;
....
328.      map = strtok_r(string, ":", &token);
```

#### Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=772">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=772</a>
Status	New

The variable declared in token at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c in line 291 is not initialized when it is used by map at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c in line 291.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	295	339
Object	token	map

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method parse\_endpoints(tcpr\_cidrmap\_t \*\*cidrmap1, tcpr\_cidrmap\_t \*\*cidrmap2, const char \*optarg)

```
....  
295.      char *token = NULL;  
....  
339.      map = strtok_r(NULL, ":", &token);
```

#### Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=773">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=773</a>
Status	New

The variable declared in cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c in line 365 is not initialized when it is used by cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	367	389
Object	cidr	cidr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.         tcpr_cidr_t *cidr = NULL;  
....  
389.         ptr->to = cidr->next;
```

#### Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=774">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=774</a>
Status	New

The variable declared in cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c in line 365 is not initialized when it is used by cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	367	409
Object	cidr	cidr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.         tcpr_cidr_t *cidr = NULL;  
....  
409.         ptr->to = cidr->next;
```

#### Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=775">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=775</a>
Status	New

The variable declared in token at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c in line 291 is not initialized when it is used by map at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c in line 291.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	295	328
Object	token	map



**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27785-FP.c  
Method parse\_endpoints(tcp\_r\_cidrmap\_t \*\*cidrmap1, tcp\_r\_cidrmap\_t \*\*cidrmap2, const char \*optarg)

```
....  
295.         char *token = NULL;  
....  
328.         map = strtok_r(string, ":", &token);
```

**Use of Zero Initialized Pointer\Path 13:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=776>  
Status New

The variable declared in token at vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27785-FP.c in line 291 is not initialized when it is used by map at vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27785-FP.c in line 291.

	Source	Destination
File	vul_files_1_1/appneta@@tcp replay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcp replay-v4.5.0-CVE-2023-27785-FP.c
Line	295	339
Object	token	map

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27785-FP.c  
Method parse\_endpoints(tcp\_r\_cidrmap\_t \*\*cidrmap1, tcp\_r\_cidrmap\_t \*\*cidrmap2, const char \*optarg)

```
....  
295.         char *token = NULL;  
....  
339.         map = strtok_r(NULL, ":", &token);
```

**Use of Zero Initialized Pointer\Path 14:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=777>  
Status New

The variable declared in cidr at vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27785-FP.c in line 365 is not initialized when it is used by cidr at vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27785-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	367	389
Object	cidr	cidr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method parse\_cidr\_map(tcp\_r\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.      tcp_r_cidr_t *cidr = NULL;  
....  
389.      ptr->to = cidr->next;
```

#### Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=778">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=778</a>
Status	New

The variable declared in cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c in line 365 is not initialized when it is used by cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	367	409
Object	cidr	cidr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method parse\_cidr\_map(tcp\_r\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.      tcp_r_cidr_t *cidr = NULL;  
....  
409.      ptr->to = cidr->next;
```

#### Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=779">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=779</a>
Status	New

The variable declared in token at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 291 is not initialized when it is used by map at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 291.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	295	328
Object	token	map

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method parse\_endpoints(tcpr\_cidrmap\_t \*\*cidrmap1, tcpr\_cidrmap\_t \*\*cidrmap2, const char \*optarg)

```
....  
295.      char *token = NULL;  
....  
328.      map = strtok_r(string, ":", &token);
```

#### Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=780">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=780</a>
Status	New

The variable declared in token at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 291 is not initialized when it is used by map at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 291.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	295	339
Object	token	map

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method parse\_endpoints(tcpr\_cidrmap\_t \*\*cidrmap1, tcpr\_cidrmap\_t \*\*cidrmap2, const char \*optarg)

```
....  
295.      char *token = NULL;  
....  
339.      map = strtok_r(NULL, ":", &token);
```

#### Use of Zero Initialized Pointer\Path 18:

Severity	Medium
----------	--------

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=781">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=781</a>
Status	New

The variable declared in cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 365 is not initialized when it is used by cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	367	389
Object	cidr	cidr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.      tcpr_cidr_t *cidr = NULL;  
....  
389.      ptr->to = cidr->next;
```

#### Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=782">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=782</a>
Status	New

The variable declared in cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 365 is not initialized when it is used by cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	367	409
Object	cidr	cidr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....
367.         tcpr_cidr_t *cidr = NULL;
....
409.         ptr->to = cidr->next;
```

#### Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=783">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=783</a>
Status	New

The variable declared in token at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 291 is not initialized when it is used by map at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 291.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	295	328
Object	token	map

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method parse\_endpoints(tcpr\_cidrmap\_t \*\*cidrmap1, tcpr\_cidrmap\_t \*\*cidrmap2, const char \*optarg)

```
....
295.         char *token = NULL;
....
328.         map = strtok_r(string, ":", &token);
```

#### Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=784">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=784</a>
Status	New

The variable declared in token at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 291 is not initialized when it is used by map at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 291.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	295	339

Object	token	map
--------	-------	-----

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method parse\_endpoints(tcpr\_cidrmap\_t \*\*cidrmap1, tcpr\_cidrmap\_t \*\*cidrmap2, const char \*optarg)

```
....  
295.         char *token = NULL;  
....  
339.         map = strtok_r(NULL, ":", &token);
```

#### Use of Zero Initialized Pointer\Path 22:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=785>  
Status New

The variable declared in cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 365 is not initialized when it is used by cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	367	389
Object	cidr	cidr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.         tcpr_cidr_t *cidr = NULL;  
....  
389.         ptr->to = cidr->next;
```

#### Use of Zero Initialized Pointer\Path 23:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=786>  
Status New

The variable declared in cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 365 is not initialized when it is used by cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c
Line	367	409
Object	cidr	cidr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c  
Method parse\_cidr\_map(tcp\_r\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....
367.         tcp_r_cidr_t *cidr = NULL;
....
409.         ptr->to = cidr->next;
```

#### Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=787">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=787</a>
Status	New

The variable declared in token at vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c in line 291 is not initialized when it is used by map at vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c in line 291.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c
Line	295	328
Object	token	map

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27789-FP.c  
Method parse\_endpoints(tcp\_r\_cidrmap\_t \*\*cidrmap1, tcp\_r\_cidrmap\_t \*\*cidrmap2, const char \*optarg)

```
....
295.         char *token = NULL;
....
328.         map = strtok_r(string, ":", &token);
```

#### Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=788">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=788</a>
Status	New

The variable declared in token at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c in line 291 is not initialized when it is used by map at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c in line 291.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	295	339
Object	token	map

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method parse\_endpoints(tcpr\_cidrmap\_t \*\*cidrmap1, tcpr\_cidrmap\_t \*\*cidrmap2, const char \*optarg)

```
....  
295.      char *token = NULL;  
....  
339.      map = strtok_r(NULL, ":", &token);
```

#### Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=789">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=789</a>
Status	New

The variable declared in cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c in line 365 is not initialized when it is used by cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	367	389
Object	cidr	cidr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.      tcpr_cidr_t *cidr = NULL;  
....  
389.      ptr->to = cidr->next;
```

#### Use of Zero Initialized Pointer\Path 27:

Severity	Medium
----------	--------



Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=790">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=790</a>
Status	New

The variable declared in cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c in line 365 is not initialized when it is used by cidr at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	367	409
Object	cidr	cidr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.         tcpr_cidr_t *cidr = NULL;  
....  
409.         ptr->to = cidr->next;
```

#### Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=791">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=791</a>
Status	New

The variable declared in closed\_prev at vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c in line 1288 is not initialized when it is used by dep\_stream at vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c in line 1009.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c
Line	1310	1043
Object	closed_prev	dep_stream

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c  
Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....  
1310.     stream->closed_prev = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c  
Method nhttp2\_stream \*nhttp2\_session\_open\_stream(nhttp2\_session \*session,

```
....
1043.      dep_stream = nhttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

### Use of Zero Initialized Pointer\Path 29:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=792>  
Status New

The variable declared in closed\_next at vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c in line 1288 is not initialized when it is used by dep\_stream at vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c in line 1009.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c
Line	1311	1043
Object	closed_next	dep_stream

### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c  
Method void nhttp2\_session\_detach\_idle\_stream(nhttp2\_session \*session,

```
....
1311.      stream->closed_next = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c  
Method nhttp2\_stream \*nhttp2\_session\_open\_stream(nhttp2\_session \*session,

```
....
1043.      dep_stream = nhttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

### Use of Zero Initialized Pointer\Path 30:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=793>  
Status New

The variable declared in `closed_prev` at `vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c</code>
Line	1310	1043
Object	<code>closed_prev</code>	<code>dep_stream</code>

#### Code Snippet

File Name `vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c`

Method `void nhttp2_session_detach_idle_stream(nhttp2_session *session,`

```
....  
1310.     stream->closed_prev = NULL;
```



File Name `vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c`

Method `nhttp2_stream *nhttp2_session_open_stream(nhttp2_session *session,`

```
....  
1043.     dep_stream = nhttp2_session_get_stream_raw(session,  
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 31:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=794>

Status New

The variable declared in `closed_next` at `vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c</code>
Line	1311	1043
Object	<code>closed_next</code>	<code>dep_stream</code>

#### Code Snippet

File Name `vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c`

Method `void nhttp2_session_detach_idle_stream(nhttp2_session *session,`

```
....
1311.      stream->closed_next = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c  
Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.      dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

### Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=795">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=795</a>
Status	New

The variable declared in closed\_prev at vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c in line 1288 is not initialized when it is used by dep\_stream at vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c in line 1009.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c
Line	1310	1043
Object	closed_prev	dep_stream

### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c  
Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1310.      stream->closed_prev = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c  
Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.      dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

### Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=795">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=795</a>

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=796">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=796</a>
Status	New

The variable declared in `closed_next` at `vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c</code>
Line	1311	1043
Object	<code>closed_next</code>	<code>dep_stream</code>

#### Code Snippet

File Name `vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c`  
 Method `void nghttp2_session_detach_idle_stream(nghttp2_session *session,`

```
....
1311.     stream->closed_next = NULL;
```



File Name `vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c`  
 Method `nghttp2_stream *nghttp2_session_open_stream(nghttp2_session *session,`

```
....
1043.     dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=797">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=797</a>
Status	New

The variable declared in `closed_prev` at `vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c</code>
Line	1310	1043
Object	<code>closed_prev</code>	<code>dep_stream</code>

#### Code Snippet

File Name `vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c`

Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....  
1310.     stream->closed_prev = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c

Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....  
1043.     dep_stream = nghttp2_session_get_stream_raw(session,  
pri_spec->stream_id);
```

### Use of Zero Initialized Pointer\Path 35:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=798>

Status New

The variable declared in closed\_next at vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c in line 1288 is not initialized when it is used by dep\_stream at vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c in line 1009.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c
Line	1311	1043
Object	closed_next	dep_stream

### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c

Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....  
1311.     stream->closed_next = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c

Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....  
1043.     dep_stream = nghttp2_session_get_stream_raw(session,  
pri_spec->stream_id);
```

### Use of Zero Initialized Pointer\Path 36:

Severity Medium

Result State To Verify

Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=799">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=799</a>
Status	New

The variable declared in `closed_prev` at `vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c</code>
Line	1310	1043
Object	<code>closed_prev</code>	<code>dep_stream</code>

#### Code Snippet

File Name `vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c`  
 Method `void nhttp2_session_detach_idle_stream(nhttp2_session *session,`

```
....
1310.     stream->closed_prev = NULL;
```

File Name `vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c`  
 Method `nhttp2_stream *nhttp2_session_open_stream(nhttp2_session *session,`

```
....
1043.     dep_stream = nhttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=800">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=800</a>
Status	New

The variable declared in `closed_next` at `vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c</code>
Line	1311	1043
Object	<code>closed_next</code>	<code>dep_stream</code>

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c  
Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1311.     stream->closed_next = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c  
Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.     dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

### Use of Zero Initialized Pointer\Path 38:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=801>  
Status New

The variable declared in closed\_prev at vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c in line 1288 is not initialized when it is used by dep\_stream at vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c in line 1009.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c
Line	1310	1043
Object	closed_prev	dep_stream

### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c  
Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1310.     stream->closed_prev = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c  
Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.     dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

### Use of Zero Initialized Pointer\Path 39:

Severity Medium



Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=802">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=802</a>
Status	New

The variable declared in `closed_next` at `vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c</code>
Line	1311	1043
Object	<code>closed_next</code>	<code>dep_stream</code>

#### Code Snippet

File Name `vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c`  
Method `void nghttp2_session_detach_idle_stream(nghttp2_session *session,`

```
....  
1311.     stream->closed_next = NULL;
```

File Name `vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c`  
Method `nghttp2_stream *nghttp2_session_open_stream(nghttp2_session *session,`

```
....  
1043.     dep_stream = nghttp2_session_get_stream_raw(session,  
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=803">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=803</a>
Status	New

The variable declared in `closed_prev` at `vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c</code>
Line	1310	1043
Object	<code>closed_prev</code>	<code>dep_stream</code>

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c

Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1310.     stream->closed_prev = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c

Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.     dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 41:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=804>

Status New

The variable declared in closed\_next at vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c in line 1288 is not initialized when it is used by dep\_stream at vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c in line 1009.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c
Line	1311	1043
Object	closed_next	dep_stream

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c

Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1311.     stream->closed_next = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c

Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.     dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=805">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=805</a>
Status	New

The variable declared in `closed_prev` at `vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c</code>
Line	1310	1043
Object	<code>closed_prev</code>	<code>dep_stream</code>

#### Code Snippet

File Name `vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c`  
Method `void nhttp2_session_detach_idle_stream(nhttp2_session *session,`

```
....  
1310.     stream->closed_prev = NULL;
```

File Name `vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c`  
Method `nhttp2_stream *nhttp2_session_open_stream(nhttp2_session *session,`

```
....  
1043.     dep_stream = nhttp2_session_get_stream_raw(session,  
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=806">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=806</a>
Status	New

The variable declared in `closed_next` at `vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c</code>
Line	1311	1043
Object	<code>closed_next</code>	<code>dep_stream</code>

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c  
Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1311.     stream->closed_next = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c  
Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.     dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=807">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=807</a>
Status	New

The variable declared in closed\_prev at vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c in line 1288 is not initialized when it is used by dep\_stream at vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c in line 1009.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c
Line	1310	1043
Object	closed_prev	dep_stream

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c  
Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1310.     stream->closed_prev = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c  
Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.     dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

**Use of Zero Initialized Pointer\Path 45:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=808">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=808</a>
Status	New

The variable declared in `closed_next` at `vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c</code>
Line	1311	1043
Object	<code>closed_next</code>	<code>dep_stream</code>

**Code Snippet**

File Name `vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c`  
Method `void nghttp2_session_detach_idle_stream(nghttp2_session *session,`

```
....  
1311.     stream->closed_next = NULL;
```

File Name `vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c`  
Method `nghttp2_stream *nghttp2_session_open_stream(nghttp2_session *session,`

```
....  
1043.     dep_stream = nghttp2_session_get_stream_raw(session,  
pri_spec->stream_id);
```

**Use of Zero Initialized Pointer\Path 46:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=809">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=809</a>
Status	New

The variable declared in `closed_prev` at `vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c</code>
Line	1310	1043

Object	closed_prev	dep_stream
--------	-------------	------------

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c  
Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1310.     stream->closed_prev = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c  
Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.     dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=810">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=810</a>
Status	New

The variable declared in closed\_next at vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c in line 1288 is not initialized when it is used by dep\_stream at vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c in line 1009.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c
Line	1311	1043
Object	closed_next	dep_stream

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c  
Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1311.     stream->closed_next = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c  
Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.      dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=811">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=811</a>
Status	New

The variable declared in `closed_prev` at `vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c` in line 1009.

	Source	Destination
File	<code>vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c</code>	<code>vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c</code>
Line	1310	1043
Object	<code>closed_prev</code>	<code>dep_stream</code>

#### Code Snippet

File Name `vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c`  
Method `void nghttp2_session_detach_idle_stream(nghttp2_session *session,`

```
....
1310.      stream->closed_prev = NULL;
```

File Name `vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c`  
Method `nghttp2_stream *nghttp2_session_open_stream(nghttp2_session *session,`

```
....
1043.      dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=812">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=812</a>
Status	New

The variable declared in `closed_next` at `vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c` in line 1288 is not initialized when it is used by `dep_stream` at `vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c` in line 1009.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c
Line	1311	1043
Object	closed_next	dep_stream

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c  
Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1311.     stream->closed_next = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c  
Method nghttp2\_stream \*nghttp2\_session\_open\_stream(nghttp2\_session \*session,

```
....
1043.     dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

#### Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=813">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=813</a>
Status	New

The variable declared in closed\_prev at vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c in line 1288 is not initialized when it is used by dep\_stream at vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c in line 1009.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c
Line	1310	1043
Object	closed_prev	dep_stream

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c  
Method void nghttp2\_session\_detach\_idle\_stream(nghttp2\_session \*session,

```
....
1310.     stream->closed_prev = NULL;
```

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c



Method `nghttp2_stream *nghttp2_session_open_stream(nghttp2_session *session,`

```
....
1043.         dep_stream = nghttp2_session_get_stream_raw(session,
pri_spec->stream_id);
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=125">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=125</a>
Status	New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

### Code Snippet

File Name `vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c`

Method `static int session_new(nghttp2_session **session_ptr,`

```
....
495.         sizeof((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=126">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=126</a>
Status	New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can

enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c  
Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.                sizeof ((*session_ptr)->user_recv_ext_types));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=127">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=127</a>
Status	New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c  
Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.                sizeof ((*session_ptr)->user_recv_ext_types));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=128">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=128</a>
Status	New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c

Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.          sizeof((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=129>

Status New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c

Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.          sizeof((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=130>

Status New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c

Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.          sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=131>

Status New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c

Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.          sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=132>

Status New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c

Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.          sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=133>

Status New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c

Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.          sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=133>

Status [pathid=134](#)  
New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c  
Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.          sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=135>  
Status New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c  
Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.          sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 12:

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

[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=136](http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=136)

Status New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2024-28182-TP.c  
Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.          sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=137>  
Status New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.13-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.13-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.13-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.13-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.13-CVE-2020-11080-TP.c  
Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.          sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity Medium  
Result State To Verify



Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=138">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=138</a>
Status	New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.13-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.13-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.13-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.13-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.13-CVE-2024-28182-TP.c  
Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.                sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=139">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=139</a>
Status	New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2020-11080-TP.c  
Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.                sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
----------	--------



Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=140">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=140</a>
Status	New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2024-28182-TP.c  
Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.                sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=141">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=141</a>
Status	New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.3.1-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.3.1-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.3.1-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.3.1-CVE-2020-11080-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.3.1-CVE-2020-11080-TP.c  
Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.                sizeof ((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=142">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=142</a>
Status	New

The size of the buffer used by session\_new in session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.3.1-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_new passes to session\_ptr, at line 403 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.3.1-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.3.1-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.3.1-CVE-2024-28182-TP.c
Line	495	495
Object	session_ptr	session_ptr

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.3.1-CVE-2024-28182-TP.c

Method static int session\_new(nghttp2\_session \*\*session\_ptr,

```
....  
495.             sizeof((*session_ptr)->user_recv_ext_types));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=143">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=143</a>
Status	New

The size of the buffer used by new\_cidr in tcpr\_cidr\_t, at line 98 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new\_cidr passes to tcpr\_cidr\_t, at line 98 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	104	104
Object	tcpr_cidr_t	tcpr_cidr_t

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c

Method new\_cidr(void)

```
....  
104.             memset(newcidr, '\0', sizeof(tcpr_cidr_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 20:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=144">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=144</a>
Status	New

The size of the buffer used by new\_cidr\_map in tcpr\_cidrmap\_t, at line 115 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new\_cidr\_map passes to tcpr\_cidrmap\_t, at line 115 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	121	121
Object	tcpr_cidrmap_t	tcpr_cidrmap_t

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method new\_cidr\_map(void)

```
....  
121.      memset(new, '\0', sizeof(tcpr_cidrmap_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 21:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=145">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=145</a>
Status	New

The size of the buffer used by new\_cidr in tcpr\_cidr\_t, at line 98 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new\_cidr passes to tcpr\_cidr\_t, at line 98 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	104	104
Object	tcpr_cidr_t	tcpr_cidr_t

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method new\_cidr(void)

```
....
104.      memset(newcidr, '\0', sizeof(tcpr_cidr_t));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=146">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=146</a>
Status	New

The size of the buffer used by new\_cidr\_map in tcpr\_cidrmap\_t, at line 115 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new\_cidr\_map passes to tcpr\_cidrmap\_t, at line 115 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	121	121
Object	tcpr_cidrmap_t	tcpr_cidrmap_t

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method new\_cidr\_map(void)

```
....
121.      memset(new, '\0', sizeof(tcpr_cidrmap_t));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=147">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=147</a>
Status	New

The size of the buffer used by new\_cidr in tcpr\_cidr\_t, at line 98 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new\_cidr passes to tcpr\_cidr\_t, at line 98 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	104	104
Object	tcpr_cidr_t	tcpr_cidr_t

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c  
Method new\_cidr(void)

```
....  
104.      memset(newcidr, '\0', sizeof(tcpr_cidr_t));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=148>  
Status New

The size of the buffer used by new\_cidr\_map in tcpr\_cidrmap\_t, at line 115 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new\_cidr\_map passes to tcpr\_cidrmap\_t, at line 115 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c
Line	121	121
Object	tcpr_cidrmap_t	tcpr_cidrmap_t

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27786-FP.c  
Method new\_cidr\_map(void)

```
....  
121.      memset(new, '\0', sizeof(tcpr_cidrmap_t));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=149>  
Status New

The size of the buffer used by new\_cidr in tcpr\_cidr\_t, at line 98 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new\_cidr passes to tcpr\_cidr\_t, at line 98 of vul\_files\_1\_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27787-FP.c
Line	104	104
Object	tcpr_cidr_t	tcpr_cidr_t

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method new\_cidr(void)

```
....  
104.      memset(newcidr, '\0', sizeof(tcpr_cidr_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 26:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=150>  
Status New

The size of the buffer used by new\_cidr\_map in tcpr\_cidrmap\_t, at line 115 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new\_cidr\_map passes to tcpr\_cidrmap\_t, at line 115 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	121	121
Object	tcpr_cidrmap_t	tcpr_cidrmap_t

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method new\_cidr\_map(void)

```
....  
121.      memset(new, '\0', sizeof(tcpr_cidrmap_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 27:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=151>  
Status New

The size of the buffer used by new\_cidr in tcpr\_cidr\_t, at line 98 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new\_cidr passes to tcpr\_cidr\_t, at line 98 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c

Line	104	104
Object	tcpr_cidr_t	tcpr_cidr_t

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method new\_cidr(void)

```
....
104.      memset(newcidr, '\0', sizeof(tcpr_cidr_t));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=152">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=152</a>
Status	New

The size of the buffer used by new\_cidr\_map in tcpr\_cidrmap\_t, at line 115 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that new\_cidr\_map passes to tcpr\_cidrmap\_t, at line 115 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	121	121
Object	tcpr_cidrmap_t	tcpr_cidrmap_t

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method new\_cidr\_map(void)

```
....
121.      memset(new, '\0', sizeof(tcpr_cidrmap_t));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=153">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=153</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nhttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nhttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c, to overwrite the target buffer.



	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
363.     memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=154">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=154</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
364.     memset(&iframe->ext_frame_payload, 0,  
sizeof(nghttp2_ext_frame_payload));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=155">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=155</a>
Status	New



The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
363.     memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=156">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=156</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2024-28182-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
364.     memset(&iframe->ext_frame_payload, 0,  
sizeof(nghttp2_ext_frame_payload));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=156">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=156</a>

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=157">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=157</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....
363.     memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=158">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=158</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....
364.     memset(&iframe->ext_frame_payload, 0,
sizeof(nghttp2_ext_frame_payload));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 35:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=159">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=159</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

**Code Snippet**

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
363.     memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 36:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=160">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=160</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

**Code Snippet**

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2024-28182-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....
364.     memset(&iframe->ext_frame_payload, 0,
sizeof(nghhttp2_ext_frame_payload));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=161">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=161</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghhttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghhttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....
363.     memset(&iframe->frame, 0, sizeof(nghhttp2_frame));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=162">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=162</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghhttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghhttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

## Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nghhttp2\_session \*session) {

```
....  
364.     memset(&iframe->ext_frame_payload, 0,  
sizeof(nghhttp2_ext_frame_payload));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 39:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=163>  
Status New

The size of the buffer used by session\_inbound\_frame\_reset in nghhttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghhttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

## Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c  
Method static void session\_inbound\_frame\_reset(nghhttp2\_session \*session) {

```
....  
363.     memset(&iframe->frame, 0, sizeof(nghhttp2_frame));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 40:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=164>  
Status New

The size of the buffer used by session\_inbound\_frame\_reset in nghhttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghhttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-	vul_files_1_1/arangodb@@arangodb-

	v3.10.9-CVE-2024-28182-TP.c	v3.10.9-CVE-2024-28182-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2024-28182-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
364.     memset(&iframe->ext_frame_payload, 0,  
sizeof(nghttp2_ext_frame_payload));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=165>  
Status New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
363.     memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=166>  
Status New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that

session\_inbound\_frame\_reset passes to nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
364.     memset(&iframe->ext_frame_payload, 0,  
sizeof(nghttp2_ext_frame_payload));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=167>  
Status New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
363.     memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=168>  
Status New



The size of the buffer used by session\_inbound\_frame\_reset in nhttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nhttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c
Line	364	364
Object	nhttp2_ext_frame_payload	nhttp2_ext_frame_payload

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2024-28182-TP.c  
Method static void session\_inbound\_frame\_reset(nhttp2\_session \*session) {

```
....  
364.     memset(&iframe->ext_frame_payload, 0,  
sizeof(nhttp2_ext_frame_payload));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=169">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=169</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nhttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nhttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c
Line	363	363
Object	nhttp2_frame	nhttp2_frame

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nhttp2\_session \*session) {

```
....  
363.     memset(&iframe->frame, 0, sizeof(nhttp2_frame));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify



Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=170">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=170</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
364.     memset(&iframe->ext_frame_payload, 0,  
sizeof(nghttp2_ext_frame_payload));
```

#### Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=171">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=171</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
363.     memset(&iframe->frame, 0, sizeof(nghttp2_frame));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 48:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=172">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=172</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

**Code Snippet**

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2024-28182-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....  
364.     memset(&iframe->ext_frame_payload, 0,  
sizeof(nghttp2_ext_frame_payload));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 49:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=173">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=173</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghttp2\_frame, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c
Line	363	363
Object	nghttp2_frame	nghttp2_frame

**Code Snippet**

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c  
Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....
363.     memset(&iframe->frame, 0, sizeof(nghhttp2_frame));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=174">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=174</a>
Status	New

The size of the buffer used by session\_inbound\_frame\_reset in nghhttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that session\_inbound\_frame\_reset passes to nghhttp2\_ext\_frame\_payload, at line 298 of vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c, to overwrite the target buffer.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c	vul_files_1_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c
Line	364	364
Object	nghttp2_ext_frame_payload	nghttp2_ext_frame_payload

### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.0-alpha.2-CVE-2020-11080-TP.c  
 Method static void session\_inbound\_frame\_reset(nghttp2\_session \*session) {

```
....
364.     memset(&iframe->ext_frame_payload, 0,
sizeof(nghhttp2_ext_frame_payload));
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=605">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=605</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpplay-v4.5.0-CVE-2023-27784-FP.c

Line	117	117
Object	neW	neW

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c

Method new\_cidr\_map(void)

```
....  
117.      tcpr_cidrmap_t *new;
```

**Memory Leak\Path 2:**

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=606>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	117	117
Object	neW	neW

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c

Method new\_cidr\_map(void)

```
....  
117.      tcpr_cidrmap_t *new;
```

**Memory Leak\Path 3:**

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=607>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	117	117
Object	neW	neW

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c

Method new\_cidr\_map(void)

```
....  
117.      tcpr_cidrmap_t *new;
```

#### Memory Leak\Path 4:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=608>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	117	117
Object	neW	neW

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c

Method new\_cidr\_map(void)

```
....  
117.      tcpr_cidrmap_t *new;
```

#### Memory Leak\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=609>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	117	117
Object	neW	neW

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c

Method new\_cidr\_map(void)

```
....  
117.      tcpr_cidrmap_t *new;
```

#### Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=610">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=610</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=611">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=611</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

#### Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=612">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=612</a>

Status	New
--------	-----

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c  
 Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
50.         if ((ptr = malloc(len)) == NULL) {
```

#### Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=613">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=613</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c  
 Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....
95.         if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

#### Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=614">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=614</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-	vul_files_1_1/appneta@@tcpreplay-

	v4.3.3-beta1-CVE-2023-27786-TP.c	v4.3.3-beta1-CVE-2023-27786-TP.c
Line	50	50
Object	ptr	ptr

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c

Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

**Memory Leak\Path 11:**

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=615>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	95	95
Object	newstr	newstr

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c

Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

**Memory Leak\Path 12:**

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=616>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	50	50
Object	ptr	ptr



## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

**Memory Leak\Path 13:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=617>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	95	95
Object	newstr	newstr

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

**Memory Leak\Path 14:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=618>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	50	50
Object	ptr	ptr

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

**Memory Leak\Path 15:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=619">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=619</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	95	95
Object	newstr	newstr

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

**Memory Leak\Path 16:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=620">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=620</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c
Line	50	50
Object	ptr	ptr

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

**Memory Leak\Path 17:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=621">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=621</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c
Line	95	95
Object	newstr	newstr

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.         if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

**Memory Leak\Path 18:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=622">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=622</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c
Line	50	50
Object	ptr	ptr

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.         if ((ptr = malloc(len)) == NULL) {
```

**Memory Leak\Path 19:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=623">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=623</a>

[pathid=623](#)

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c
Line	95	95
Object	newstr	newstr

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c

Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

**Memory Leak\Path 20:**

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=624>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c
Line	50	50
Object	ptr	ptr

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c

Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

**Memory Leak\Path 21:**

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=625>

Status New

Source	Destination
--------	-------------

File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c

Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

#### Memory Leak\Path 22:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=626>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c

Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Memory Leak\Path 23:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=627>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c
Line	95	95

Object	newstr	newstr
--------	--------	--------

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.         if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

#### Memory Leak\Path 24:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=628>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.         if ((ptr = malloc(len)) == NULL) {
```

#### Memory Leak\Path 25:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=629>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c

Method `_our_safe_strdup(const char *str, const char *funcname, const int line, const char *file)`

```
....  
95.         if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

### Memory Leak\Path 26:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=630>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c

Method `_our_safe_malloc(size_t len, const char *funcname, const int line, const char *file)`

```
....  
50.         if ((ptr = malloc(len)) == NULL) {
```

### Memory Leak\Path 27:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=631>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c

Method `_our_safe_strdup(const char *str, const char *funcname, const int line, const char *file)`

```
....  
95.         if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

### Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=632">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=632</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.         if ((ptr = malloc(len)) == NULL) {
```

### Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=633">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=633</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.         if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```



**Memory Leak\Path 30:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=634">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=634</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c
Line	50	50
Object	ptr	ptr

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

**Memory Leak\Path 31:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=635">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=635</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c
Line	95	95
Object	newstr	newstr

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

**Memory Leak\Path 32:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=636">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=636</a>

Status	<a href="#">pathid=636</a> New
--------	-----------------------------------

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c

Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Memory Leak\Path 33:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=637>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c

Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

#### Memory Leak\Path 34:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=638>

Status New

Source	Destination
--------	-------------

File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Memory Leak\Path 35:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=639>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

#### Memory Leak\Path 36:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=640>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c
Line	50	50

Object	ptr	ptr
--------	-----	-----

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Memory Leak\Path 37:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=641>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

#### Memory Leak\Path 38:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=642>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c

Method `_our_safe_malloc(size_t len, const char *funcname, const int line, const char *file)`

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

### Memory Leak\Path 39:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=643>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c

Method `_our_safe_strdup(const char *str, const char *funcname, const int line, const char *file)`

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

### Memory Leak\Path 40:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=644>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c

Method `_our_safe_malloc(size_t len, const char *funcname, const int line, const char *file)`

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

### Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=645">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=645</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

### Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=646">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=646</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c
Line	50	50
Object	ptr	ptr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

**Memory Leak\Path 43:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=647">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=647</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c
Line	95	95
Object	newstr	newstr

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

**Memory Leak\Path 44:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=648">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=648</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c
Line	50	50
Object	ptr	ptr

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

**Memory Leak\Path 45:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=649">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=649</a>

Status [pathid=649](#)  
New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c
Line	95	95
Object	newstr	newstr

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
95.      if ((newstr = (char *)malloc(strlen(str) + 1)) == NULL) {
```

#### Memory Leak\Path 46:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=650>  
Status New

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-14397-FP.c  
Method intern\_regions (unw\_addr\_space\_t as, unw\_accessors\_t \*a,

```
....  
73.      region = calloc (1, _U_dyn_region_info_size (op_count));
```

#### Memory Leak\Path 47:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=651>  
Status New

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-	vul_files_1_1/arangodb@@arangodb-



	v3.10.12-CVE-2020-14397-FP.c	v3.10.12-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-14397-FP.c  
Method intern\_regions (unw\_addr\_space\_t as, unw\_accessors\_t \*a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

#### Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=652">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=652</a>
Status	New

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-14397-FP.c  
Method intern\_regions (unw\_addr\_space\_t as, unw\_accessors\_t \*a,

```
....
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

#### Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=653">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=653</a>
Status	New

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-14397-FP.c  
Method intern\_regions (unw\_addr\_space\_t as, unw\_accessors\_t \*a,

```
....  
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

### Memory Leak\Path 50:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=654>  
Status New

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-14397-FP.c
Line	73	73
Object	region	region

### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-14397-FP.c  
Method intern\_regions (unw\_addr\_space\_t as, unw\_accessors\_t \*a,

```
....  
73.    region = calloc (1, _U_dyn_region_info_size (op_count));
```

## 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=1000012&projectid=7&pathid=230>  
Status New

The function len in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c at line 46 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	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	50	50
Object	len	len

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27784-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

**Wrong Size t Allocation\Path 2:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=231>  
Status New

The function len in vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27785-TP.c at line 46 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	vul_files_1_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	50	50
Object	len	len

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27785-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

**Wrong Size t Allocation\Path 3:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=232>  
Status New

The function len in vul\_files\_1\_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27786-TP.c at line 46 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	vul_files_1_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcp replay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	50	50

Object	len	len
--------	-----	-----

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c

Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 4:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=233>

Status New

The function len in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c at line 46 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	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	50	50
Object	len	len

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c

Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=234>

Status New

The function len in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c at line 46 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	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	50	50
Object	len	len

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c  
 Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

### Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=235">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=235</a>
Status	New

The function len in vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c at line 46 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	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c
Line	50	50
Object	len	len

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c  
 Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

### Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=236">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=236</a>
Status	New

The function `len` in `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c` at line 46 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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c</code>
Line	50	50
Object	<code>len</code>	<code>len</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c`

Method `_our_safe_malloc(size_t len, const char *funcname, const int line, const char *file)`

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 8:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=237>

Status New

The function `len` in `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c` at line 46 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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c</code>
Line	50	50
Object	<code>len</code>	<code>len</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c`

Method `_our_safe_malloc(size_t len, const char *funcname, const int line, const char *file)`

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 9:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=237>

Status [pathid=238](#)  
New

The function len in vul\_files\_1\_1/appneta@@tcpplay-v4.3.4-beta1-CVE-2023-27787-FP.c at line 46 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	vul_files_1_1/appneta@@tcpplay-v4.3.4-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpplay-v4.3.4-beta1-CVE-2023-27787-FP.c
Line	50	50
Object	len	len

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.3.4-beta1-CVE-2023-27787-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 10:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=239>  
Status New

The function len in vul\_files\_1\_1/appneta@@tcpplay-v4.3.4-beta1-CVE-2023-27789-FP.c at line 46 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	vul_files_1_1/appneta@@tcpplay-v4.3.4-beta1-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpplay-v4.3.4-beta1-CVE-2023-27789-FP.c
Line	50	50
Object	len	len

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpplay-v4.3.4-beta1-CVE-2023-27789-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 11:

Severity Medium

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=240">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=240</a>
Status	New

The function `len` in `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c` at line 46 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	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c</code>
Line	50	50
Object	<code>len</code>	<code>len</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c`  
Method `_our_safe_malloc(size_t len, const char *funcname, const int line, const char *file)`

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=241">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=241</a>
Status	New

The function `len` in `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c` at line 46 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	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c</code>
Line	50	50
Object	<code>len</code>	<code>len</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c`  
Method `_our_safe_malloc(size_t len, const char *funcname, const int line, const char *file)`

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```



**Wrong Size t Allocation\Path 13:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=242">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=242</a>
Status	New

The function `len` in `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c` at line 46 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	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c</code>
Line	50	50
Object	<code>len</code>	<code>len</code>

**Code Snippet**

File Name `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c`  
Method `_our_safe_malloc(size_t len, const char *funcname, const int line, const char *file)`

```
...  
50.      if ((ptr = malloc(len)) == NULL) {
```

**Wrong Size t Allocation\Path 14:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=243">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=243</a>
Status	New

The function `len` in `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c` at line 46 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	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c</code>
Line	50	50
Object	<code>len</code>	<code>len</code>

**Code Snippet**

File Name `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c`  
Method `_our_safe_malloc(size_t len, const char *funcname, const int line, const char *file)`

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

### Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=244">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=244</a>
Status	New

The function len in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c at line 46 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	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c
Line	50	50
Object	len	len

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

### Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=245">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=245</a>
Status	New

The function len in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c at line 46 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	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c
Line	50	50
Object	len	len

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 17:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=246>  
Status New

The function len in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c at line 46 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	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c
Line	50	50
Object	len	len

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 18:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=247>  
Status New

The function len in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c at line 46 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	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c
Line	50	50

Object	len	len
--------	-----	-----

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c  
 Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=248">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=248</a>
Status	New

The function len in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c at line 46 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	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c
Line	50	50
Object	len	len

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c  
 Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

#### Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=249">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=249</a>
Status	New

The function len in vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c at line 46 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	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c
Line	50	50
Object	len	len

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c  
 Method `_our_safe_malloc(size_t len, const char *funcname, const int line, const char *file)`

```
....
50.      if ((ptr = malloc(len)) == NULL) {
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=600">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=600</a>
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.0-alpha.1-CVE-2020-14397-FP.c  
 Method `intern_array (unw_addr_space_t as, unw_accessors_t *a,`

```
....
122.      free (data);
```

#### MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=601">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=601</a>
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.10.12-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.12-CVE-2020-14397-FP.c  
Method intern\_array (unw\_addr\_space\_t as, unw\_accessors\_t \*a,

```
....  
122.      free (data);
```

#### MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=602">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=602</a>
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.10.9-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.10.9-CVE-2020-14397-FP.c  
Method intern\_array (unw\_addr\_space\_t as, unw\_accessors\_t \*a,

```
....  
122.      free (data);
```

#### MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=603">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=603</a>
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.11.10-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.11.10-CVE-2020-14397-FP.c  
Method intern\_array (unw\_addr\_space\_t as, unw\_accessors\_t \*a,

```
....
122.      free (data);
```

#### MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=604">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=604</a>
Status	New

Calling free() (line 100) on a variable that was not dynamically allocated (line 100) in file vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-14397-FP.c may result with a crash.

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.12.0-CVE-2020-14397-FP.c
Line	122	122
Object	data	data

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.12.0-CVE-2020-14397-FP.c  
Method intern\_array (unw\_addr\_space\_t as, unw\_accessors\_t \*a,

```
....
122.      free (data);
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=985">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=985</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	247	247
Object	fgets	fgets

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
247.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### **Improper Resource Access Authorization\Path 2:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=986">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=986</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	247	247
Object	fgets	fgets

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
247.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### **Improper Resource Access Authorization\Path 3:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=987">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=987</a>



Status	New
--------	-----

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	247	247
Object	fgets	fgets

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
247.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=988">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=988</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	245	245
Object	fgets	fgets

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
245.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=989">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=989</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c

Line	245	245
Object	fgets	fgets

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
245.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### Improper Resource Access Authorization\Path 6:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=990>

Status New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	233	233
Object	fgets	fgets

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
233.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### Improper Resource Access Authorization\Path 7:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=991>

Status New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	233	233
Object	fgets	fgets

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
233.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### Improper Resource Access Authorization\Path 8:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=992>

Status New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	247	247
Object	line	line

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
247.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### Improper Resource Access Authorization\Path 9:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=993>

Status New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	247	247
Object	line	line

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
247.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=994">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=994</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	247	247
Object	line	line

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
247.      while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=995">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=995</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	245	245
Object	line	line

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
245.      while (fgets(line, LINE_MAX, fs) != NULL) {
```

#### Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=996">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=996</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	245	245
Object	line	line

**Code Snippet**

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
245.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

**Improper Resource Access Authorization\Path 13:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=997>  
Status New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	233	233
Object	line	line

**Code Snippet**

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
233.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

**Improper Resource Access Authorization\Path 14:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=998>  
Status New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	233	233

Object	line	line
--------	------	------

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
233.         while (fgets(line, LINE_MAX, fs) != NULL) {
```

### Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=999">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=999</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	51	51
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
51.         fprintf(stderr, "ERROR in %s:%s() line %d: Unable to
malloc() %zu bytes/n",
```

### Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1000">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1000</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	77	77
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c

Method `_our_safe_realloc(void *ptr, size_t len, const char *funcname, const int line, const char *file)`

```
....  
77.          fprintf(stderr, "ERROR: in %s:%s() line %d: Unable to  
remalloc() buffer to %zu bytes", file, funcname, line, len);
```

#### Improper Resource Access Authorization\Path 17:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1001>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	96	96
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c  
Method `_our_safe_strdup(const char *str, const char *funcname, const int line, const char *file)`

```
....  
96.          fprintf(stderr, "ERROR in %s:%s() line %d: Unable to  
strdup() %zu bytes\n", file, funcname, line, strlen(str));
```

#### Improper Resource Access Authorization\Path 18:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1002>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	132	132
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c  
Method `u_char *_our_safe_pcap_next(pcap_t *pcap, struct pcap_pkthdr *pkthdr,`

```
....  
132.                fprintf(stderr, "safe_pcap_next ERROR: Invalid packet  
length in %s:%s() line %d: %u is greater than maximum %u\n",
```

### Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1003">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1003</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	138	138
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c  
Method u\_char \*\_our\_safe\_pcap\_next(pcap\_t \*pcap, struct pcap\_pkthdr \*pkthdr,

```
....  
138.                fprintf(stderr, "safe_pcap_next ERROR: Invalid packet  
length in %s:%s() line %d: packet length=%u capture length=%u\n",
```

### Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1004">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1004</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	168	168
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c  
Method int \_our\_safe\_pcap\_next\_ex(pcap\_t \*pcap, struct pcap\_pkthdr \*\*pkthdr,

```
....  
168.                fprintf(stderr, "safe_pcap_next_ex ERROR: Invalid  
packet length in %s:%s() line %d: %u is greater than maximum %u\n",
```



**Improper Resource Access Authorization\Path 21:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1005">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1005</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c
Line	174	174
Object	fprintf	fprintf

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27784-TP.c

Method int \_our\_safe\_pcap\_next\_ex(pcap\_t \*pcap, struct pcap\_pkthdr \*\*pkthdr,

```
....  
174.          fprintf(stderr, "safe_pcap_next_ex ERROR: Invalid  
packet length in %s:%s() line %d: packet length=%u capture length=%u\n",
```

**Improper Resource Access Authorization\Path 22:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1006">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1006</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	51	51
Object	fprintf	fprintf

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c

Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
51.          fprintf(stderr, "ERROR in %s:%s() line %d: Unable to  
malloc() %zu bytes/n",
```

**Improper Resource Access Authorization\Path 23:**

Severity	Low
Result State	To Verify

Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1007">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1007</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	77	77
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c  
Method \_our\_safe\_realloc(void \*ptr, size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
77.          fprintf(stderr, "ERROR: in %s:%s() line %d: Unable to  
remalloc() buffer to %zu bytes", file, funcname, line, len);
```

### Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1008">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1008</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	96	96
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
96.          fprintf(stderr, "ERROR in %s:%s() line %d: Unable to  
strdup() %zu bytes\n", file, funcname, line, strlen(str));
```

### Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1009">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1009</a>

Status	New
--------	-----

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	132	132
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c

Method u\_char \*\_our\_safe\_pcap\_next(pcap\_t \*pcap, struct pcap\_pkthdr \*pkthdr,

```
....  
132.                fprintf(stderr, "safe_pcap_next ERROR: Invalid packet  
length in %s:%s() line %d: %u is greater than maximum %u\n",
```

#### Improper Resource Access Authorization\Path 26:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1010>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	138	138
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c

Method u\_char \*\_our\_safe\_pcap\_next(pcap\_t \*pcap, struct pcap\_pkthdr \*pkthdr,

```
....  
138.                fprintf(stderr, "safe_pcap_next ERROR: Invalid packet  
length in %s:%s() line %d: packet length=%u capture length=%u\n",
```

#### Improper Resource Access Authorization\Path 27:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1011>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-	vul_files_1_1/appneta@@tcpreplay-

	v4.3.3-beta1-CVE-2023-27785-TP.c	v4.3.3-beta1-CVE-2023-27785-TP.c
Line	168	168
Object	fprintf	fprintf

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c  
Method int \_our\_safe\_pcap\_next\_ex(pcap\_t \*pcap, struct pcap\_pkthdr \*\*pkthdr,

```
....  
168.                fprintf(stderr, "safe_pcap_next_ex ERROR: Invalid  
packet length in %s:%s() line %d: %u is greater than maximum %u\n",
```

**Improper Resource Access Authorization\Path 28:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1012">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1012</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c
Line	174	174
Object	fprintf	fprintf

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c  
Method int \_our\_safe\_pcap\_next\_ex(pcap\_t \*pcap, struct pcap\_pkthdr \*\*pkthdr,

```
....  
174.                fprintf(stderr, "safe_pcap_next_ex ERROR: Invalid  
packet length in %s:%s() line %d: packet length=%u capture length=%u\n",
```

**Improper Resource Access Authorization\Path 29:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1013">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1013</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	51	51
Object	fprintf	fprintf

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
51.          fprintf(stderr, "ERROR in %s:%s() line %d: Unable to  
malloc() %zu bytes/n",
```

**Improper Resource Access Authorization\Path 30:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1014>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	77	77
Object	fprintf	fprintf

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c  
Method \_our\_safe\_realloc(void \*ptr, size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
77.          fprintf(stderr, "ERROR: in %s:%s() line %d: Unable to  
remalloc() buffer to %zu bytes", file, funcname, line, len);
```

**Improper Resource Access Authorization\Path 31:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1015>  
Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	96	96
Object	fprintf	fprintf

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c

Method `_our_safe_strdup(const char *str, const char *funcname, const int line, const char *file)`

```
....  
96.             fprintf(stderr, "ERROR in %s:%s() line %d: Unable to  
strcpy() %zu bytes\n", file, funcname, line, strlen(str));
```

### Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1016">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1016</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	132	132
Object	fprintf	fprintf

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c`

Method `u_char *_our_safe_pcap_next(pcap_t *pcap, struct pcap_pkthdr *pkthdr,`

```
....  
132.             fprintf(stderr, "safe_pcap_next ERROR: Invalid packet  
length in %s:%s() line %d: %u is greater than maximum %u\n",
```

### Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1017">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1017</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	138	138
Object	fprintf	fprintf

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c`

Method `u_char *_our_safe_pcap_next(pcap_t *pcap, struct pcap_pkthdr *pkthdr,`

```
....  
138.                fprintf(stderr, "safe_pcap_next ERROR: Invalid packet  
length in %s:%s() line %d: packet length=%u capture length=%u\n",
```

#### Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1018">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1018</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	168	168
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c  
Method int \_our\_safe\_pcap\_next\_ex(pcap\_t \*pcap, struct pcap\_pkthdr \*\*pkthdr,

```
....  
168.                fprintf(stderr, "safe_pcap_next_ex ERROR: Invalid  
packet length in %s:%s() line %d: %u is greater than maximum %u\n",
```

#### Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1019">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1019</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c
Line	174	174
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c  
Method int \_our\_safe\_pcap\_next\_ex(pcap\_t \*pcap, struct pcap\_pkthdr \*\*pkthdr,

```
....  
174.                fprintf(stderr, "safe_pcap_next_ex ERROR: Invalid  
packet length in %s:%s() line %d: packet length=%u capture length=%u\n",
```

**Improper Resource Access Authorization\Path 36:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1020">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1020</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	51	51
Object	fprintf	fprintf

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
51.          fprintf(stderr, "ERROR in %s:%s() line %d: Unable to  
malloc() %zu bytes/n",
```

**Improper Resource Access Authorization\Path 37:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1021">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1021</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	77	77
Object	fprintf	fprintf

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c  
Method \_our\_safe\_realloc(void \*ptr, size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
77.          fprintf(stderr, "ERROR: in %s:%s() line %d: Unable to  
remalloc() buffer to %zu bytes", file, funcname, line, len);
```

**Improper Resource Access Authorization\Path 38:**

Severity	Low
----------	-----



Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1022">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1022</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	96	96
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c

Method `_our_safe_strdup(const char *str, const char *funcname, const int line, const char *file)`

```
....
96.          fprintf(stderr, "ERROR in %s:%s() line %d: Unable to
_strdup() %zu bytes\n", file, funcname, line, strlen(str));
```

### Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1023">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1023</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	132	132
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c

Method `u_char *_our_safe_pcap_next(pcap_t *pcap, struct pcap_pkthdr *pkthdr,`

```
....
132.          fprintf(stderr, "safe_pcap_next ERROR: Invalid packet
length in %s:%s() line %d: %u is greater than maximum %u\n",
```

### Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1024">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1024</a>

Status	New
--------	-----

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	138	138
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c

Method u\_char \*\_our\_safe\_pcap\_next(pcap\_t \*pcap, struct pcap\_pkthdr \*pkthdr,

```
....  
138.                fprintf(stderr, "safe_pcap_next ERROR: Invalid packet  
length in %s:%s() line %d: packet length=%u capture length=%u\n",
```

#### Improper Resource Access Authorization\Path 41:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1025>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c
Line	168	168
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c

Method int \_our\_safe\_pcap\_next\_ex(pcap\_t \*pcap, struct pcap\_pkthdr \*\*pkthdr,

```
....  
168.                fprintf(stderr, "safe_pcap_next_ex ERROR: Invalid  
packet length in %s:%s() line %d: %u is greater than maximum %u\n",
```

#### Improper Resource Access Authorization\Path 42:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1026>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-	vul_files_1_1/appneta@@tcpreplay-

	v4.3.3-beta1-CVE-2023-27787-FP.c	v4.3.3-beta1-CVE-2023-27787-FP.c
Line	174	174
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c

Method int \_our\_safe\_pcap\_next\_ex(pcap\_t \*pcap, struct pcap\_pkthdr \*\*pkthdr,

```
....  
174.             fprintf(stderr, "safe_pcap_next_ex ERROR: Invalid  
packet length in %s:%s() line %d: packet length=%u capture length=%u\n",
```

#### Improper Resource Access Authorization\Path 43:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1027>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	51	51
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c

Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
51.             fprintf(stderr, "ERROR in %s:%s() line %d: Unable to  
malloc() %zu bytes/n",
```

#### Improper Resource Access Authorization\Path 44:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1028>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	77	77

Object	fprintf	fprintf
--------	---------	---------

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c  
Method \_our\_safe\_realloc(void \*ptr, size\_t len, const char \*funcname, const int line, const char \*file)

```
....  
77.          fprintf(stderr, "ERROR: in %s:%s() line %d: Unable to  
remalloc() buffer to %zu bytes", file, funcname, line, len);
```

#### Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1029">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1029</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	96	96
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c  
Method \_our\_safe\_strdup(const char \*str, const char \*funcname, const int line, const char \*file)

```
....  
96.          fprintf(stderr, "ERROR in %s:%s() line %d: Unable to  
strdup() %zu bytes\n", file, funcname, line, strlen(str));
```

#### Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1030">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1030</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	132	132
Object	fprintf	fprintf

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c

Method u\_char \*\_our\_safe\_pcap\_next(pcap\_t \*pcap, struct pcap\_pkthdr \*pkthdr,

```
....  
132.                fprintf(stderr, "safe_pcap_next ERROR: Invalid packet  
length in %s:%s() line %d: %u is greater than maximum %u\n",
```

**Improper Resource Access Authorization\Path 47:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1031>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	138	138
Object	fprintf	fprintf

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c

Method u\_char \*\_our\_safe\_pcap\_next(pcap\_t \*pcap, struct pcap\_pkthdr \*pkthdr,

```
....  
138.                fprintf(stderr, "safe_pcap_next ERROR: Invalid packet  
length in %s:%s() line %d: packet length=%u capture length=%u\n",
```

**Improper Resource Access Authorization\Path 48:**

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1032>

Status New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	168	168
Object	fprintf	fprintf

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c

Method int \_our\_safe\_pcap\_next\_ex(pcap\_t \*pcap, struct pcap\_pkthdr \*\*pkthdr,

```
....  
168.                fprintf(stderr, "safe_pcap_next_ex ERROR: Invalid  
packet length in %s:%s() line %d: %u is greater than maximum %u\n",
```

#### Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1033">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1033</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c
Line	174	174
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c  
Method int \_our\_safe\_pcap\_next\_ex(pcap\_t \*pcap, struct pcap\_pkthdr \*\*pkthdr,

```
....  
174.                fprintf(stderr, "safe_pcap_next_ex ERROR: Invalid  
packet length in %s:%s() line %d: packet length=%u capture length=%u\n",
```

#### Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1034">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1034</a>
Status	New

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c
Line	51	51
Object	fprintf	fprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c  
Method \_our\_safe\_malloc(size\_t len, const char \*funcname, const int line, const char \*file)

```
....
51.          fprintf(stderr, "ERROR in %s:%s() line %d: Unable to
malloc() %zu bytes/n",
```

## NULL Pointer Dereference

Query Path:

CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

### Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

OWASP Top 10 2017: A1-Injection

### Description

#### NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=702">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=702</a>
Status	New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	279	104
Object	null	regex_text

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.          i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
104.      pcre_free_substring(i->regex_text);
```

#### NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=702">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=702</a>

	<a href="http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=703">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=703</a>
Status	New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	279	103
Object	null	regex_text

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.             i = NULL;
```



File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
103.     if (i->regex_text) {
```

#### NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=704">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=704</a>
Status	New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	279	101
Object	null	regex

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)



```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
101.        pcre_free(i->regex);
```

#### NULL Pointer Dereference\Path 4:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=705>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	279	100
Object	null	regex

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
100.        if (i->regex) {
```

#### NULL Pointer Dereference\Path 5:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=706>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	279	95
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.             i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
95.         pcre_free(i->regex_extra);
```

#### NULL Pointer Dereference\Path 6:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=707>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	279	93
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
93.    if (i->regex_extra) {
```

### NULL Pointer Dereference\Path 7:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=708>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	279	104
Object	null	regex_text

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
104.    pcre_free_substring(i->regex_text);
```

### NULL Pointer Dereference\Path 8:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=709>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	279	103
Object	null	regex_text

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.          i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
103.    if (i->regex_text) {
```

#### NULL Pointer Dereference\Path 9:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=710>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	279	101
Object	null	regex

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
101.        pcre_free(i->regex);
```

### NULL Pointer Dereference\Path 10:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=711>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	279	100
Object	null	regex

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
100.        if (i->regex) {
```

### NULL Pointer Dereference\Path 11:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=712>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	279	95
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
279.          i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....  
95.      pcre_free(i->regex_extra);
```

#### NULL Pointer Dereference\Path 12:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=713>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	279	93
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
93.    if (i->regex_extra) {
```

### NULL Pointer Dereference\Path 13:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=714>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	279	104
Object	null	regex_text

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
104.    pcre_free_substring(i->regex_text);
```

### NULL Pointer Dereference\Path 14:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=715>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	279	103
Object	null	regex_text

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.             i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
103.     if (i->regex_text) {
```

#### NULL Pointer Dereference\Path 15:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=716>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	279	101
Object	null	regex

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)



```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
101.        pcre_free(i->regex);
```

### NULL Pointer Dereference\Path 16:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=717>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	279	100
Object	null	regex

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
100.        if (i->regex) {
```

### NULL Pointer Dereference\Path 17:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=718>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	279	95
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.             i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
95.         pcre_free(i->regex_extra);
```

#### NULL Pointer Dereference\Path 18:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=719>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 215 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c in line 91.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	279	93
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
279.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
93.    if (i->regex_extra) {
```

### NULL Pointer Dereference\Path 19:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=720>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	277	102
Object	null	regex_text

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
102.    pcre_free_substring(i->regex_text);
```

### NULL Pointer Dereference\Path 20:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=721>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	277	101
Object	null	regex_text

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.             i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
101.     if (i->regex_text) {
```

#### NULL Pointer Dereference\Path 21:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=722>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	277	99
Object	null	regex

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
99.                pcre_free(i->regex);
```

### NULL Pointer Dereference\Path 22:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=723>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	277	98
Object	null	regex

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
98.        if (i->regex) {
```

### NULL Pointer Dereference\Path 23:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=724>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	277	93
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.             i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
93.         pcre_free(i->regex_extra);
```

#### NULL Pointer Dereference\Path 24:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=725>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	277	91
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
91.    if (i->regex_extra) {
```

### NULL Pointer Dereference\Path 25:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=726>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	277	102
Object	null	regex_text

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
102.    pcre_free_substring(i->regex_text);
```

### NULL Pointer Dereference\Path 26:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=727>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	277	101
Object	null	regex_text

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.             i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
101.     if (i->regex_text) {
```

#### NULL Pointer Dereference\Path 27:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=728>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	277	99
Object	null	regex

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)



```
....
277.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
99.                pcre_free(i->regex);
```

### NULL Pointer Dereference\Path 28:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=729>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	277	98
Object	null	regex

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
98.        if (i->regex) {
```

### NULL Pointer Dereference\Path 29:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=730>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	277	93
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
93.        pcre_free(i->regex_extra);
```

#### NULL Pointer Dereference\Path 30:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=731>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 213 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c in line 89.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	277	91
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
277.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
91.    if (i->regex_extra) {
```

### NULL Pointer Dereference\Path 31:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=732>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	265	90
Object	null	regex_text

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
90.    pcre_free_substring(i->regex_text);
```

### NULL Pointer Dereference\Path 32:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=733>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	265	89
Object	null	regex_text

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.          i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c

Method free\_invalidate\_t(invalidate\_t \*i)

```
....
89.    if (i->regex_text) {
```

#### NULL Pointer Dereference\Path 33:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=734>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	265	87
Object	null	regex

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
87.                pcre_free(i->regex);
```

### NULL Pointer Dereference\Path 34:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=735>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	265	86
Object	null	regex

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
86.        if (i->regex) {
```

### NULL Pointer Dereference\Path 35:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=736>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	265	81
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.             i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
81.         pcre_free(i->regex_extra);
```

#### NULL Pointer Dereference\Path 36:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=737>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	265	79
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
79.    if (i->regex_extra) {
```

### NULL Pointer Dereference\Path 37:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=738>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	265	90
Object	null	regex_text

### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
90.    pcre_free_substring(i->regex_text);
```

### NULL Pointer Dereference\Path 38:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=739>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex\_text at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	265	89
Object	null	regex_text

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.             i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
89.     if (i->regex_text) {
```

#### NULL Pointer Dereference\Path 39:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=740>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	265	87
Object	null	regex

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)



```
....
265.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
87.                pcre_free(i->regex);
```

#### NULL Pointer Dereference\Path 40:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=741>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	265	86
Object	null	regex

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
86.        if (i->regex) {
```

#### NULL Pointer Dereference\Path 41:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=742>

Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	265	81
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.             i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
81.         pcre_free(i->regex_extra);
```

#### NULL Pointer Dereference\Path 42:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=743>  
Status New

The variable declared in null at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 201 is not initialized when it is used by regex\_extra at vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c in line 77.

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	265	79
Object	null	regex_extra

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
265.                i = NULL;
```

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method free\_invalidate\_t(invalidate\_t \*i)

```
....
79.    if (i->regex_extra) {
```

### NULL Pointer Dereference\Path 43:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=744>  
Status New

The variable declared in null at vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27784-FP.c in line 365 is not initialized when it is used by next at vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27784-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcp replay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcp replay-v4.5.0-CVE-2023-27784-FP.c
Line	367	402
Object	null	next

### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27784-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....
367.    tcpr_cidr_t *cidr = NULL;
....
402.    if (cidr->next == NULL)
```

### NULL Pointer Dereference\Path 44:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=745>  
Status New

The variable declared in null at vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27784-FP.c in line 365 is not initialized when it is used by next at vul\_files\_1\_1/appneta@@tcp replay-v4.5.0-CVE-2023-27784-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	367	381
Object	null	next

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method parse\_cidr\_map(tcp\_r\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.      tcp_r_cidr_t *cidr = NULL;  
....  
381.      if (cidr->next == NULL)
```

#### NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=746">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=746</a>
Status	New

The variable declared in null at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c in line 365 is not initialized when it is used by next at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c in line 365.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	367	402
Object	null	next

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method parse\_cidr\_map(tcp\_r\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.      tcp_r_cidr_t *cidr = NULL;  
....  
402.      if (cidr->next == NULL)
```

#### NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=747">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=747</a>
Status	New

The variable declared in null at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c in line 365 is not initialized when it is used by next at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c in line 381.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	367	381
Object	null	next

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c

Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....
367.         tcpr_cidr_t *cidr = NULL;
....
381.         if (cidr->next == NULL)
```

#### NULL Pointer Dereference\Path 47:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=748>

Status New

The variable declared in null at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 365 is not initialized when it is used by next at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 402.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	367	402
Object	null	next

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c

Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....
367.         tcpr_cidr_t *cidr = NULL;
....
402.         if (cidr->next == NULL)
```

#### NULL Pointer Dereference\Path 48:

Severity Low

Result State To Verify

Online Results <http://WIN->

[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=749](http://PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=749)

Status New

The variable declared in null at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 365 is not initialized when it is used by next at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c in line 381.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c
Line	367	381
Object	null	next

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.      tcpr_cidr_t *cidr = NULL;  
....  
381.      if (cidr->next == NULL)
```

#### NULL Pointer Dereference\Path 49:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=750>  
Status New

The variable declared in null at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 365 is not initialized when it is used by next at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 402.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	367	402
Object	null	next

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.      tcpr_cidr_t *cidr = NULL;  
....  
402.      if (cidr->next == NULL)
```

**NULL Pointer Dereference\Path 50:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=751">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=751</a>
Status	New

The variable declared in null at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 365 is not initialized when it is used by next at vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c in line 381.

	Source	Destination
File	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	367	381
Object	null	next

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method parse\_cidr\_map(tcpr\_cidrmap\_t \*\*cidrmap, const char \*optarg)

```
....  
367.      tcpr_cidr_t *cidr = NULL;  
....  
381.      if (cidr->next == NULL)
```

**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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=655">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=655</a>
Status	New

The load\_config method calls the sprintf function, at line 215 of vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-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	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	232	232

Object	snprintf	snprintf
--------	----------	----------

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
232.      snprintf(path, path_len, "%s/%s", TSConfigDirGet(), pstate-
>config_file);
```

#### Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=656">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=656</a>
Status	New

The load\_config method calls the snprintf function, at line 215 of vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-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	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	232	232
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
232.      snprintf(path, path_len, "%s/%s", TSConfigDirGet(), pstate-
>config_file);
```

#### Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=657">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=657</a>
Status	New

The load\_config method calls the snprintf function, at line 215 of vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-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	vul_files_1_1/apache@@trafficserver-	vul_files_1_1/apache@@trafficserver-



	8.1.8-rc0-CVE-2020-14397-FP.c	8.1.8-rc0-CVE-2020-14397-FP.c
Line	232	232
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
232.      snprintf(path, path_len, "%s/%s", TSConfigDirGet(), pstate->config_file);
```

#### Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=658">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=658</a>
Status	New

The load\_config method calls the snprintf function, at line 213 of vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-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	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	230	230
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
230.      snprintf(path, path_len, "%s/%s", TSConfigDirGet(), pstate->config_file);
```

#### Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=659">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=659</a>
Status	New

The load\_config method calls the snprintf function, at line 213 of vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-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	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	230	230
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
230.      snprintf(path, path_len, "%s/%s", TSConfigDirGet(), pstate-
>config_file);
```

#### Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=660">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=660</a>
Status	New

The load\_config method calls the snprintf function, at line 201 of vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-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	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	218	218
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
218.      snprintf(path, path_len, "%s/%s", TSConfigDirGet(), pstate-
>config_file);
```

#### Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=661">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=661</a>
Status	New

The load\_config method calls the snprintf function, at line 201 of vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-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	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	218	218
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
218.      snprintf(path, path_len, "%s/%s", TSConfigDirGet(), pstate->config_file);
```

#### Unchecked Return Value\Path 8:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=662>

Status New

The httpAddrString method calls the snprintf function, at line 497 of vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-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	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	531	531
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c

Method httpAddrString(const http\_addr\_t \*addr, /\* I - Address to convert \*/

```
....  
531.      snprintf(s, (size_t)slen, "%d.%d.%d.%d", (temp >> 24) & 255,
```

#### Unchecked Return Value\Path 9:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=663>

Status New

The httpAddrString method calls the snprintf function, at line 497 of vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-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	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	634	634
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c

Method httpAddrString(const http\_addr\_t \*addr, /\* I - Address to convert \*/

```
....  
634.      snprintf(s, (size_t)slen, "[v1.%s]", temps);
```

#### Unchecked Return Value\Path 10:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=664>

Status New

The httpGetHostname method calls the snprintf function, at line 790 of vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-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	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	842	842
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c

Method httpGetHostname(http\_t \*http, /\* I - HTTP connection or NULL \*/

```
....  
842.      snprintf(s, (size_t)slen, "%s.local.", localStr);
```

#### Unchecked Return Value\Path 11:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=664>

Status [pathid=665](#)  
New

The httpAddrString method calls the snprintf function, at line 497 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-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	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c
Line	531	531
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c

Method httpAddrString(const http\_addr\_t \*addr, /\* I - Address to convert \*/

```
....  
531.      snprintf(s, (size_t)slen, "%d.%d.%d.%d", (temp >> 24) & 255,
```

#### Unchecked Return Value\Path 12:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=666>

Status New

The httpAddrString method calls the snprintf function, at line 497 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-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	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c
Line	634	634
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c

Method httpAddrString(const http\_addr\_t \*addr, /\* I - Address to convert \*/

```
....  
634.      snprintf(s, (size_t)slen, "[v1.%s]", temps);
```

#### Unchecked Return Value\Path 13:

Severity Low

Result State To Verify

Online Results <http://WIN->

	<a href="#">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=667</a>
Status	New

The `httpGetHostname` method calls the `snprintf` function, at line 790 of `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-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	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c</code>
Line	842	842
Object	<code>snprintf</code>	<code>snprintf</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c`  
Method `httpGetHostname(http_t *http, /* I - HTTP connection or NULL */`

```
....  
842.         snprintf(s, (size_t)slen, "%s.local.", localStr);
```

#### Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	<a href="#">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=668</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpplay-v4.3.3-beta1-CVE-2023-27784-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	<code>vul_files_1_1/appneta@@tcpplay-v4.3.3-beta1-CVE-2023-27784-TP.c</code>	<code>vul_files_1_1/appneta@@tcpplay-v4.3.3-beta1-CVE-2023-27784-TP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpplay-v4.3.3-beta1-CVE-2023-27784-TP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify

Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=669">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=669</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27785-TP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=670">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=670</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27786-TP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 17:

Severity	Low
----------	-----

Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=671">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=671</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27787-FP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=672">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=672</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.3-beta1-CVE-2023-27789-TP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 19:



Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=673">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=673</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27784-FP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=674">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=674</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27785-FP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

**Unchecked Return Value\Path 21:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=675">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=675</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

**Code Snippet**

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27786-FP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

**Unchecked Return Value\Path 22:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=676">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=676</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

**Code Snippet**

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27787-FP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

**Unchecked Return Value\Path 23:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=677">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=677</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

**Code Snippet**

File Name `vul_files_1_1/appneta@@tcpreplay-v4.3.4-beta1-CVE-2023-27789-FP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

**Unchecked Return Value\Path 24:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=678">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=678</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

**Code Snippet**

File Name `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27784-FP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=679">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=679</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27785-TP.c`  
Method `int format_date_time(struct timeval *when, char *buf, size_t len)`

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=680">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=680</a>
Status	New

The `format_date_time` method calls the `snprintf` function, at line 268 of `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-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	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c</code>	<code>vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c</code>
Line	280	280
Object	<code>snprintf</code>	<code>snprintf</code>

#### Code Snippet

File Name `vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27786-FP.c`

Method int format\_date\_time(struct timeval \*when, char \*buf, size\_t len)

```
....  
280.      return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=681">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=681</a>
Status	New

The format\_date\_time method calls the snprintf function, at line 268 of vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-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	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c
Line	280	280
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27787-TP.c  
Method int format\_date\_time(struct timeval \*when, char \*buf, size\_t len)

```
....  
280.      return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=682">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=682</a>
Status	New

The format\_date\_time method calls the snprintf function, at line 268 of vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-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	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c
Line	280	280
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.2-beta1-CVE-2023-27789-FP.c  
Method int format\_date\_time(struct timeval \*when, char \*buf, size\_t len)

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 29:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=683>  
Status New

The format\_date\_time method calls the snprintf function, at line 268 of vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-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	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c
Line	280	280
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27784-TP.c  
Method int format\_date\_time(struct timeval \*when, char \*buf, size\_t len)

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

#### Unchecked Return Value\Path 30:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=684>  
Status New

The format\_date\_time method calls the snprintf function, at line 268 of vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-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	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c
Line	280	280
Object	snprintf	snprintf

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27785-TP.c  
Method int format\_date\_time(struct timeval \*when, char \*buf, size\_t len)

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

**Unchecked Return Value\Path 31:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=685>  
Status New

The format\_date\_time method calls the snprintf function, at line 268 of vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-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	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c
Line	280	280
Object	snprintf	snprintf

**Code Snippet**

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27786-TP.c  
Method int format\_date\_time(struct timeval \*when, char \*buf, size\_t len)

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

**Unchecked Return Value\Path 32:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=686>  
Status New

The format\_date\_time method calls the snprintf function, at line 268 of vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-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	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c
Line	280	280
Object	snprintf	snprintf

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27787-TP.c  
Method int format\_date\_time(struct timeval \*when, char \*buf, size\_t len)

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

**Unchecked Return Value\Path 33:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=687>  
Status New

The format\_date\_time method calls the snprintf function, at line 268 of vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-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	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c	vul_files_1_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c
Line	280	280
Object	snprintf	snprintf

## Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.4.3-CVE-2023-27789-TP.c  
Method int format\_date\_time(struct timeval \*when, char \*buf, size\_t len)

```
....  
280.         return snprintf(buf, len, tmp, when->tv_usec);
```

**Unchecked Return Value\Path 34:**

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=688>  
Status New

The cidr2cidr method calls the snprintf function, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-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	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c
Line	200	200



Object	snprintf	snprintf
--------	----------	----------

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27784-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
200.                snprintf(tempoctet, sizeof(octets[count]), "%u",  
octets[count]);
```

#### Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=689">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=689</a>
Status	New

The cidr2cidr method calls the snprintf function, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-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	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c
Line	200	200
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27785-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
200.                snprintf(tempoctet, sizeof(octets[count]), "%u",  
octets[count]);
```

#### Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=690">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=690</a>
Status	New

The cidr2cidr method calls the snprintf function, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-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	vul_files_1_1/appneta@@tcpreplay-	vul_files_1_1/appneta@@tcpreplay-

	v4.5.0-CVE-2023-27786-FP.c	v4.5.0-CVE-2023-27786-FP.c
Line	200	200
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27786-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
200.                snprintf(tempoctet, sizeof(octets[count]), "%u",  
octets[count]);
```

#### Unchecked Return Value\Path 37:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=691>  
Status New

The cidr2cidr method calls the snprintf function, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-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	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c
Line	200	200
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27787-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
200.                snprintf(tempoctet, sizeof(octets[count]), "%u",  
octets[count]);
```

#### Unchecked Return Value\Path 38:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=692>  
Status New

The cidr2cidr method calls the snprintf function, at line 132 of vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-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	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c	vul_files_1_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c
Line	200	200
Object	snprintf	snprintf

#### Code Snippet

File Name vul\_files\_1\_1/appneta@@tcpreplay-v4.5.0-CVE-2023-27789-FP.c  
Method cidr2cidr(char \*cidr)

```
....  
200.          snprintf(tempoctet, sizeof(octets[count]), "%u",  
octets[count]);
```

## 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	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1190">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1190</a>
Status	New

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	223	223
Object	chmod	chmod

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c  
Method httpAddrListen(http\_addr\_t \*addr, /\* I - Address to bind to \*/

```
....  
223.          chmod(addr->un.sun_path, 0140777);
```

#### Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1190">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1190</a>

Status	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1191">PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1191</a> New
--------	---

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c
Line	223	223
Object	chmod	chmod

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c  
Method httpAddrListen(http\_addr\_t \*addr, /\* I - Address to bind to \*/

```
....  
223.      chmod(addr->un.sun_path, 0140777);
```

### Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1192">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1192</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	242	242
Object	fs	fs

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
242.      if (!(fs = fopen(path, "r"))) {
```

### Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1193">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1193</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-	vul_files_1_1/apache@@trafficserver-

	8.1.3-rc0-CVE-2020-14397-FP.c	8.1.3-rc0-CVE-2020-14397-FP.c
Line	242	242
Object	fs	fs

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
242.      if (!(fs = fopen(path, "r"))) {
```

#### Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1194">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1194</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	242	242
Object	fs	fs

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
242.      if (!(fs = fopen(path, "r"))) {
```

#### Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1195">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1195</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	240	240
Object	fs	fs

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
240.      if (!(fs = fopen(path, "r"))) {
```

#### Incorrect Permission Assignment For Critical Resources\Path 7:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1196>  
Status New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	240	240
Object	fs	fs

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
240.      if (!(fs = fopen(path, "r"))) {
```

#### Incorrect Permission Assignment For Critical Resources\Path 8:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1197>  
Status New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	228	228
Object	fs	fs

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
228.      if (!(fs = fopen(path, "r"))) {
```

**Incorrect Permission Assignment For Critical Resources\Path 9:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1198">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1198</a>
Status	New

	Source	Destination
File	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	228	228
Object	fs	fs

**Code Snippet**

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
228.      if (!(fs = fopen(path, "r"))) {
```

**TOCTOU**

Query Path:

CPP\Cx\CPP Low Visibility\TOCTOU Version:1

**Description****TOCTOU\Path 1:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1199">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1199</a>
Status	New

The load\_config method in vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.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	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c
Line	242	242
Object	fopen	fopen

**Code Snippet**

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.2-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
242.      if (!(fs = fopen(path, "r"))) {
```

**TOCTOU\Path 2:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1200">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1200</a>
Status	New

The load\_config method in vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.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	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c
Line	242	242
Object	fopen	fopen

**Code Snippet**

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.3-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
242.      if (!(fs = fopen(path, "r"))) {
```

**TOCTOU\Path 3:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1201">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1201</a>
Status	New

The load\_config method in vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.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	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c
Line	242	242
Object	fopen	fopen

**Code Snippet**

File Name vul\_files\_1\_1/apache@@trafficserver-8.1.8-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)



```
....  
242.      if (!(fs = fopen(path, "r"))) {
```

#### TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1202">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1202</a>
Status	New

The load\_config method in vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.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	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c
Line	240	240
Object	fopen	fopen

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.0-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
240.      if (!(fs = fopen(path, "r"))) {
```

#### TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1203">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=1203</a>
Status	New

The load\_config method in vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.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	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c
Line	240	240
Object	fopen	fopen

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.0.1-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
240.      if (!(fs = fopen(path, "r"))) {
```

#### TOCTOU\Path 6:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1204>

Status New

The load\_config method in vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.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	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c
Line	228	228
Object	fopen	fopen

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.2-rc0-CVE-2020-14397-FP.c

Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....  
228.      if (!(fs = fopen(path, "r"))) {
```

#### TOCTOU\Path 7:

Severity Low

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=1205>

Status New

The load\_config method in vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.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	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c	vul_files_1_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c
Line	228	228
Object	fopen	fopen

#### Code Snippet

File Name vul\_files\_1\_1/apache@@trafficserver-9.1.4-rc0-CVE-2020-14397-FP.c  
Method load\_config(plugin\_state\_t \*pstate, invalidate\_t \*\*ilist)

```
....
228.      if (!(fs = fopen(path, "r"))) {
```

## Reliance on DNS Lookups in a Decision

Query Path:

CPP\Cx\CPP Low Visibility\Reliance on DNS Lookups in a Decision Version:0

### Categories

FISMA 2014: Identification And Authentication  
NIST SP 800-53: SC-23 Session Authenticity (P1)

### Description

#### Reliance on DNS Lookups in a Decision\Path 1:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=696">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=696</a>
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c. The application then makes a security decision, error, in vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c
Line	387	391
Object	getnameinfo	error

### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c  
Method httpAddrLookup(

```
....
387.      int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
391.      if (error == EAI_FAIL)
```

#### Reliance on DNS Lookups in a Decision\Path 2:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=697">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=697</a>
Status	New

The `httpAddrLookup` method performs a reverse DNS lookup with `getnameinfo`, at line 315 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`. The application then makes a security decision, `==`, in `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c` line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	387	391
Object	<code>getnameinfo</code>	<code>==</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`  
Method `httpAddrLookup(`

```
....  
387.      int error = getnameinfo(&addr->addr,  
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);  
....  
391.      if (error == EAI_FAIL)
```

#### Reliance on DNS Lookups in a Decision\Path 3:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=698">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=698</a>
Status	New

The `httpAddrLookup` method performs a reverse DNS lookup with `getnameinfo`, at line 315 of `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`. The application then makes a security decision, `error`, in `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c` line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>	<code>vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c</code>
Line	387	389
Object	<code>getnameinfo</code>	<code>error</code>

#### Code Snippet

File Name `vul_files_1_1/apple@@cups-v2.3.3-CVE-2024-35235-TP.c`  
Method `httpAddrLookup(`

```
....  
387.      int error = getnameinfo(&addr->addr,  
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);  
....  
389.      if (error)
```

#### Reliance on DNS Lookups in a Decision\Path 4:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=699">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=699</a>
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c. The application then makes a security decision, error, in vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c
Line	387	391
Object	getnameinfo	error

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c  
Method httpAddrLookup(

```
....
387.      int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
391.      if (error == EAI_FAIL)
```

#### Reliance on DNS Lookups in a Decision\Path 5:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=700">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=700</a>
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c. The application then makes a security decision, ==, in vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c
Line	387	391
Object	getnameinfo	==

#### Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c

Method httpAddrLookup(

```
....
387.         int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
391.         if (error == EAI_FAIL)
```

## Reliance on DNS Lookups in a Decision\Path 6:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=701">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=701</a>
Status	New

The httpAddrLookup method performs a reverse DNS lookup with getnameinfo, at line 315 of vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c. The application then makes a security decision, error, in vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c line 315, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c	vul_files_1_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c
Line	387	389
Object	getnameinfo	error

## Code Snippet

File Name vul\_files\_1\_1/apple@@cups-v2.3.6-CVE-2024-35235-TP.c  
Method httpAddrLookup(

```
....
387.         int error = getnameinfo(&addr->addr,
(socklen_t)httpAddrLength(addr), name, (socklen_t)namelen, NULL, 0, 0);
....
389.         if (error)
```

## Unreleased Resource Leak

Query Path:  
CPP\Cx\CPP Low Visibility\Unreleased Resource Leak Version:0

## Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

## Description

### Unreleased Resource Leak\Path 1:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=693">http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&amp;projectid=7&amp;pathid=693</a>
Status	New

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.13-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.7.13-CVE-2020-14397-FP.c
Line	928	928
Object	info	info

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.13-CVE-2020-14397-FP.c  
Method background\_thread\_boot1(tsdn\_t \*tsdn) {

```
....  
928.                if (pthread_cond_init(&info->cond, NULL)) {
```

#### Unreleased Resource Leak\Path 2:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=694>  
Status New

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2020-14397-FP.c
Line	928	928
Object	info	info

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.1-rc.1-CVE-2020-14397-FP.c  
Method background\_thread\_boot1(tsdn\_t \*tsdn) {

```
....  
928.                if (pthread_cond_init(&info->cond, NULL)) {
```

#### Unreleased Resource Leak\Path 3:

Severity Low  
Result State To Verify  
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000012&projectid=7&pathid=695>  
Status New

	Source	Destination
File	vul_files_1_1/arangodb@@arangodb-v3.7.3.1-CVE-2020-14397-FP.c	vul_files_1_1/arangodb@@arangodb-v3.7.3.1-CVE-2020-14397-FP.c
Line	928	928

Object	info	info
--------	------	------

#### Code Snippet

File Name vul\_files\_1\_1/arangodb@@arangodb-v3.7.3.1-CVE-2020-14397-FP.c  
Method background\_thread\_boot1(tsdn\_t \*tsdn) {

```
....  
928.                if (pthread_cond_init(&info->cond, NULL)) {
```

## Buffer Overflow LongString

### Risk

#### What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

### Cause

#### How does it happen

Buffer Overflows can manifest in numerous different variations. In its 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 cpycat

## 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 its 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 unbounded

## 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 its 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 (strlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

# Buffer Overflow StrcpyStrcat

## 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 its most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

---

## General Recommendations

### How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
  - Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
  - Consistently apply tests for the size of buffers.
  - Do not return variable addresses outside the scope of their variables.
- 

## Source Code Examples

# Buffer Overflow boundcpy WrongSizeParam

## Risk

### What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

---

## Cause

### How does it happen

Buffer Overflows can manifest in numerous different variations. In its 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

# 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);
```

# 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;  
}
```

**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
<a href="#">CVE-2005-3119</a>	Memory leak because function does not free() an element of a data structure.
<a href="#">CVE-2004-0427</a>	Memory leak when counter variable is not decremented.
<a href="#">CVE-2002-0574</a>	Memory leak when counter variable is not decremented.
<a href="#">CVE-2005-3181</a>	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
<a href="#">CVE-2004-0222</a>	Memory leak via unknown manipulations as part of protocol test suite.
<a href="#">CVE-2001-0136</a>	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	<a href="#">Indicator of Poor Code Quality</a>	<b>Seven Pernicious Kingdoms (primary)700</b>
ChildOf	Category	399	<a href="#">Resource Management Errors</a>	<b>Development Concepts (primary)699</b>
ChildOf	Category	633	<a href="#">Weaknesses that Affect Memory</a>	<b>Resource-specific Weaknesses (primary)631</b>
ChildOf	Category	730	<a href="#">OWASP Top Ten 2004 Category A9 - Denial of Service</a>	<b>Weaknesses in OWASP Top Ten (2004) (primary)711</b>
ChildOf	Weakness Base	772	<a href="#">Missing Release of Resource after Effective</a>	<b>Research Concepts (primary)1000</b>

MemberOf	View	630	<a href="#">Lifetime Weaknesses Examined by SAMATE</a>	<b>Weaknesses Examined by SAMATE (primary) 630</b> Research Concepts1000
CanFollow	Weakness Class	390	<a href="#">Detection of Error Condition Without Action</a>	

## 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 updated White Box Definitions	MITRE	Internal
2009-10-29	CWE Content Team updated Modes of Introduction, Other Notes	MITRE	Internal
2010-02-16	CWE Content Team updated Relationships	MITRE	Internal
<b>Previous Entry Names</b>			
<b>Change Date</b>	<b>Previous Entry Name</b>		
2008-04-11	Memory Leak		
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')		

[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



# 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 function. These functions often return error codes in the result, or share other status codes with its 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';
```

## Resource Locking Problems

**Category ID:** 411 (Category)

**Status:** Draft

### Description

### Description Summary

Weaknesses in this category are related to improper handling of locks that are used to control access to resources.

### Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	399	<a href="#">Resource Management Errors</a>	<b>Development Concepts (primary)699</b>
ParentOf	Weakness Base	412	<a href="#">Unrestricted Externally Accessible Lock</a>	Development Concepts699
ParentOf	Weakness Base	413	<a href="#">Insufficient Resource Locking</a>	<b>Development Concepts (primary)699</b>
ParentOf	Weakness Base	414	<a href="#">Missing Lock Check</a>	<b>Development Concepts (primary)699</b>

### Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Resource Locking problems

### Content History

Submissions			
Submission Date	Submitter	Organization	Source
	PLOVER		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		

[BACK TO TOP](#)

# Reliance on DNS Lookups in a Decision

## Risk

### What might happen

Relying on reverse DNS records, without verifying domain ownership via cryptographic certificates or protocols, is not a sufficient authentication mechanism. Basing any security decisions on the registered hostname could allow an external attacker to control the application flow. The attacker could possibly perform restricted operations, bypass access controls, and even spoof the user's identity, inject a bogus hostname into the security log, and possibly other logic attacks.

---

## Cause

### How does it happen

The application performs a reverse DNS resolution, based on the remote IP address, and performs a security check based on the returned hostname. However, it is relatively easy to spoof DNS names, or cause them to be misreported, depending on the context of the specific environment. If the remote server is controlled by the attacker, it can be configured to report a bogus hostname. Additionally, the attacker could also spoof the hostname if she controls the associated DNS server, or by attacking the legitimate DNS server, or by poisoning the server's DNS cache, or by modifying unprotected DNS traffic to the server. Regardless of the vector, a remote attacker can alter the detected network address, faking the authentication details.

---

## General Recommendations

### How to avoid it

- Do not rely on DNS records, network addresses, or system hostnames as a form of authentication, or any other security-related decision.
  - Do not perform reverse DNS resolution over an unprotected protocol without record validation.
  - Implement a proper authentication mechanism, such as passwords, cryptographic certificates, or public key digital signatures.
  - Consider using proposed protocol extensions to cryptographically protect DNS, e.g. DNSSEC (though note the limited support and other drawbacks).
- 

## Source Code Examples

### Java

#### Using Reverse DNS as Authentication

```
private boolean isInternalEmployee(ServletRequest req) {
    boolean isCompany = false;

    String ip = req.getRemoteAddr();
    InetAddress address = InetAddress.getByName(ip);

    if (address.getHostName().endsWith(COMPANYNAME)) {
        isCompany = true;
    }

    return isCompany;
}
```

```
}
```

### Verify Authenticated User's Identity

```
private boolean isInternalEmployee(HttpServletRequest req) {  
    boolean isCompany = false;  
  
    Principal user = req.getUserPrincipal();  
    if (user != null) {  
        if (user.getName().startsWith(COMPANYDOMAIN + "\\\")) {  
            isCompany = true;  
        }  
    }  
    return isCompany;  
}
```

# 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

### 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());
```



**Improper Access Control (Authorization)****Weakness ID:** 285 (*Weakness Class*)**Status:** Draft**Description****Description Summary**

The software does not perform or incorrectly performs access control checks across all potential execution paths.

**Extended Description**

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

**Alternate Terms****AuthZ:**

"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

**Time of Introduction**

- Architecture and Design
- Implementation
- Operation

**Applicable Platforms****Languages**

Language-independent

**Technology Classes**

Web-Server: (*Often*)

Database-Server: (*Often*)

**Modes of Introduction**

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

**Common Consequences**

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

**Likelihood of Exploit**

High

**Detection Methods**

### **Automated Static Analysis**

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

### ***Effectiveness: Limited***

---

### **Automated Dynamic Analysis**

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

---

### **Manual Analysis**

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

### ***Effectiveness: Moderate***

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

---

## **Demonstrative Examples**

### **Example 1**

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that `LookupMessageObject()` ensures that the `$id` argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

*(Bad Code)*

#### ***Example Language: Perl***

```
sub DisplayPrivateMessage {
my($id) = @_ ;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users. One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

## **Observed Examples**

Reference	Description
<a href="#">CVE-2009-3168</a>	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.



<a href="#">CVE-2009-2960</a>	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
<a href="#">CVE-2009-3597</a>	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
<a href="#">CVE-2009-2282</a>	Terminal server does not check authorization for guest access.
<a href="#">CVE-2009-3230</a>	Database server does not use appropriate privileges for certain sensitive operations.
<a href="#">CVE-2009-2213</a>	Gateway uses default "Allow" configuration for its authorization settings.
<a href="#">CVE-2009-0034</a>	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
<a href="#">CVE-2008-6123</a>	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
<a href="#">CVE-2008-5027</a>	System monitoring software allows users to bypass authorization by creating custom forms.
<a href="#">CVE-2008-7109</a>	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
<a href="#">CVE-2008-3424</a>	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
<a href="#">CVE-2009-3781</a>	Content management system does not check access permissions for private files, allowing others to view those files.
<a href="#">CVE-2008-4577</a>	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
<a href="#">CVE-2008-6548</a>	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
<a href="#">CVE-2007-2925</a>	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
<a href="#">CVE-2006-6679</a>	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
<a href="#">CVE-2005-3623</a>	OS kernel does not check for a certain privilege before setting ACLs for files.
<a href="#">CVE-2005-2801</a>	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defaults ACLs from being properly applied.
<a href="#">CVE-2001-1155</a>	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	<a href="#">Security Features</a>	<b>Seven Pernicious Kingdoms (primary)700</b>
ChildOf	Weakness Class	284	<a href="#">Access Control (Authorization) Issues</a>	<b>Development Concepts (primary)699</b> <b>Research Concepts (primary)1000</b>
ChildOf	Category	721	<a href="#">OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access</a>	<b>Weaknesses in OWASP Top Ten (2007) (primary)629</b>
ChildOf	Category	723	<a href="#">OWASP Top Ten 2004 Category A2 - Broken Access Control</a>	<b>Weaknesses in OWASP Top Ten (2004) (primary)711</b>
ChildOf	Category	753	<a href="#">2009 Top 25 - Porous Defenses</a>	<b>Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750</b>
ChildOf	Category	803	<a href="#">2010 Top 25 - Porous Defenses</a>	<b>Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800</b>
ParentOf	Weakness Variant	219	<a href="#">Sensitive Data Under Web Root</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Base	551	<a href="#">Incorrect Behavior Order: Authorization Before Parsing and Canonicalization</a>	<b>Development Concepts (primary)699</b> Research Concepts1000
ParentOf	Weakness Class	638	<a href="#">Failure to Use Complete Mediation</a>	Research Concepts1000
ParentOf	Weakness Base	804	<a href="#">Guessable CAPTCHA</a>	<b>Development Concepts (primary)699</b> <b>Research Concepts (primary)1000</b>

## 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)
<a href="#">1</a>	Accessing Functionality Not Properly Constrained by ACLs	
<a href="#">13</a>	Subverting Environment Variable Values	

<a href="#">17</a>	Accessing, Modifying or Executing Executable Files
<a href="#">87</a>	Forceful Browsing
<a href="#">39</a>	Manipulating Opaque Client-based Data Tokens
<a href="#">45</a>	Buffer Overflow via Symbolic Links
<a href="#">51</a>	Poison Web Service Registry
<a href="#">59</a>	Session Credential Falsification through Prediction
<a href="#">60</a>	Reusing Session IDs (aka Session Replay)
<a href="#">77</a>	Manipulating User-Controlled Variables
<a href="#">76</a>	Manipulating Input to File System Calls
<a href="#">104</a>	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
<a href="#">CVE-2009-3482</a>	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
<a href="#">CVE-2009-3897</a>	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
<a href="#">CVE-2009-3489</a>	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
<a href="#">CVE-2009-3289</a>	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.
<a href="#">CVE-2009-0115</a>	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
<a href="#">CVE-2009-1073</a>	LDAP server stores a cleartext password in a world-readable file.
<a href="#">CVE-2009-0141</a>	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

<a href="#">CVE-2008-0662</a>	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
<a href="#">CVE-2008-0322</a>	Driver installs its device interface with "Everyone: Write" permissions.
<a href="#">CVE-2009-3939</a>	Driver installs a file with world-writable permissions.
<a href="#">CVE-2009-3611</a>	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
<a href="#">CVE-2007-6033</a>	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
<a href="#">CVE-2007-5544</a>	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
<a href="#">CVE-2005-4868</a>	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
<a href="#">CVE-2004-1714</a>	Security product uses "Everyone: Full Control" permissions for its configuration files.
<a href="#">CVE-2001-0006</a>	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
<a href="#">CVE-2002-0969</a>	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	<a href="#">Permission Issues</a>	<b>Development Concepts (primary)699</b>
ChildOf	Weakness Class	668	<a href="#">Exposure of Resource to Wrong Sphere</a>	<b>Research Concepts (primary)1000</b>
ChildOf	Category	753	<a href="#">2009 Top 25 - Porous Defenses</a>	<b>Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750</b>
ChildOf	Category	803	<a href="#">2010 Top 25 - Porous Defenses</a>	<b>Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800</b>
RequiredBy	Compound Element: Composite	689	<a href="#">Permission Race Condition During Resource Copy</a>	Research Concepts1000
ParentOf	Weakness Variant	276	<a href="#">Incorrect Default Permissions</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Variant	277	<a href="#">Insecure Inherited Permissions</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Variant	278	<a href="#">Insecure Preserved Inherited Permissions</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Variant	279	<a href="#">Incorrect Execution- Assigned Permissions</a>	<b>Research Concepts (primary)1000</b>
ParentOf	Weakness Base	281	<a href="#">Improper Preservation of Permissions</a>	<b>Research Concepts (primary)1000</b>

## Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
<a href="#">232</a>	Exploitation of Privilege/Trust	
<a href="#">1</a>	Accessing Functionality Not Properly Constrained by ACLs	
<a href="#">17</a>	Accessing, Modifying or Executing Executable Files	
<a href="#">60</a>	Reusing Session IDs (aka Session Replay)	
<a href="#">61</a>	Session Fixation	
<a href="#">62</a>	Cross Site Request Forgery (aka Session Riding)	
<a href="#">122</a>	Exploitation of Authorization	
<a href="#">180</a>	Exploiting Incorrectly Configured Access Control Security Levels	
<a href="#">234</a>	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](#)

# TOCTOU

## Risk

### What might happen

At best, a Race Condition may cause errors in accuracy, overridden 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 these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

---

## General Recommendations

### How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

---

## Source Code Examples

### Java Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
public static int counter = 0;
public static void start() throws InterruptedException {
    incrementCounter ic;
    decrementCounter dc;
    while(counter == 0) {
        counter = 0;
        ic = new incrementCounter();
        dc = new decrementCounter();
        ic.start();
        dc.start();
        ic.join();
        dc.join();
    }
    System.out.println(counter); //Will stop and return either -1 or 1 due to race
    condition over counter
}

public static class incrementCounter extends Thread {
    public void run() {
        counter++;
    }
}
```

```
}

public static class decrementCounter extends Thread {
    public void run() {
        counter--;
    }
}
```

### Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
public static int counter = 0;
public static Object lock = new Object();

public static void start() throws InterruptedException {
    incrementCounter ic;
    decrementCounter dc;
    while(counter == 0) { // because of proper locking, this condition is never false
        counter = 0;
        ic = new incrementCounter();
        dc = new decrementCounter();
        ic.start();
        dc.start();
        ic.join();
        dc.join();
    }
    System.out.println(counter); // Never reached
}

public static class incrementCounter extends Thread {
    public void run() {
        synchronized (lock) {
            counter++;
        }
    }
}

public static class decrementCounter extends Thread {
    public void run() {
        synchronized (lock) {
            counter--;
        }
    }
}
```

## Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025