vul_files_5 Scan Report

Project Name	vul_files_5
Scan Start	Monday, January 6, 2025 2:22:31 PM
Preset	Checkmarx Default
Scan Time	03h:37m:25s
Lines Of Code Scanned	299206
Files Scanned	53
Report Creation Time	Monday, January 6, 2025 6:40:22 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	3/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

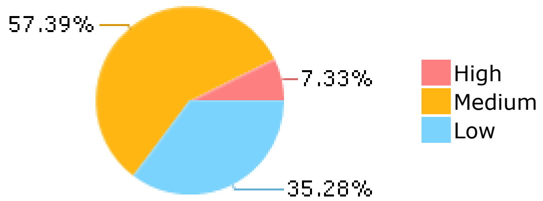
Results Limit

Results limit per query was set to 50

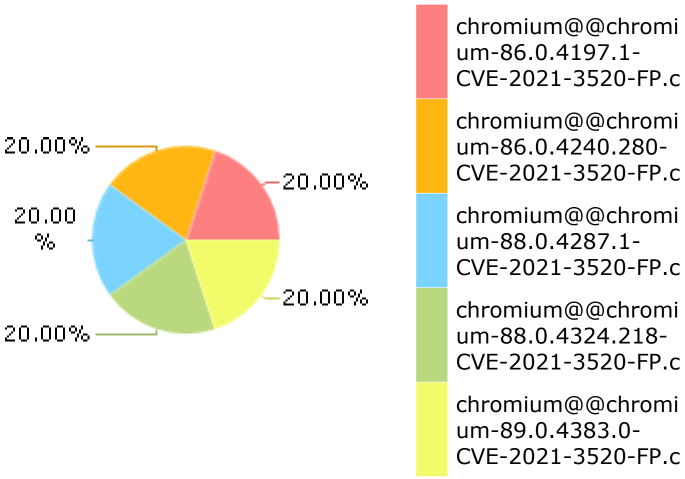
Selected Queries

Selected queries are listed in Result Summary

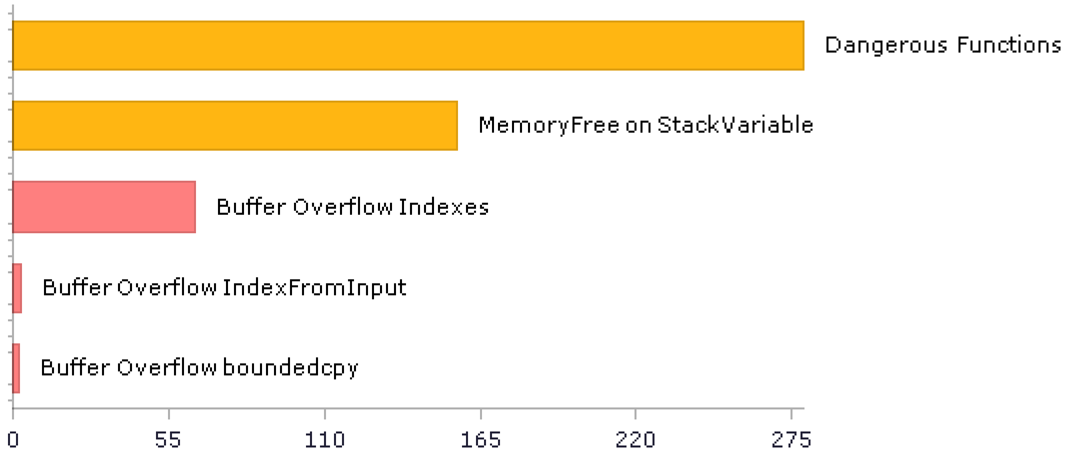
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	154	105
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	30	30
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	279	279
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	3	3
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	279	279
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	148	99
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.	19	19
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.	21	21
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.	27	27
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.	3	3

* 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)	51	51
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)*****	16	16
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)*****	24	19
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*****	69	20
SI-11 Error Handling (P2)*****	207	207
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 wasnt done correctly.	0	0
M6-Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	0	0
M8-Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

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

Scan Summary - Custom

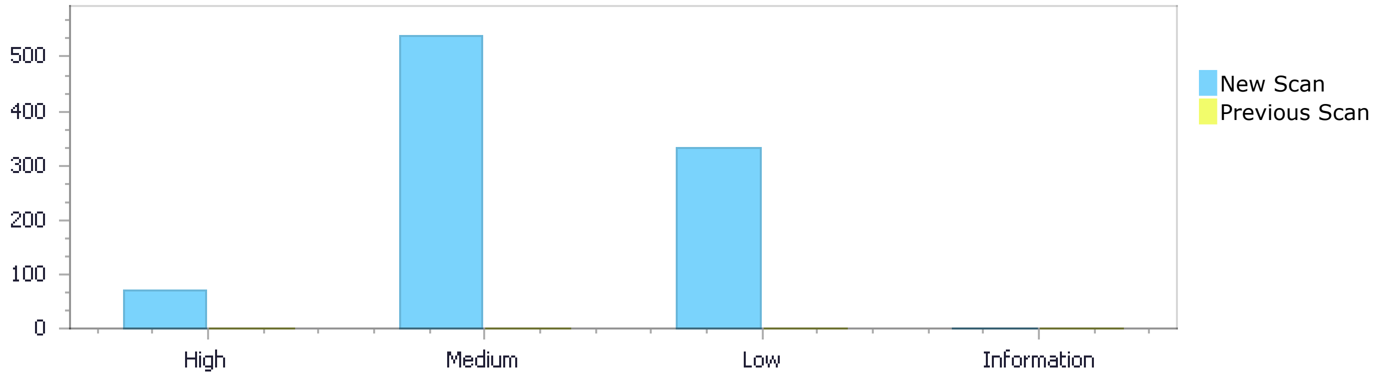
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	69	540	332	0	941
Recurrent Issues	0	0	0	0	0
Total	69	540	332	0	941

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	69	540	332	0	941
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	69	540	332	0	941

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow Indexes	64	High
Buffer Overflow IndexFromInput	3	High
Buffer Overflow boundedcpy	2	High
Dangerous Functions	279	Medium
MemoryFree on StackVariable	157	Medium

Buffer Overflow boundcpy WrongSizeParam	77	Medium
Use of Zero Initialized Pointer	10	Medium
Memory Leak	9	Medium
Buffer Overflow AddressOfLocalVarReturned	5	Medium
Environment Injection	3	Medium
Unchecked Return Value	207	Low
Sizeof Pointer Argument	32	Low
TOCTOU	23	Low
Exposure of System Data to Unauthorized Control Sphere	21	Low
Incorrect Permission Assignment For Critical Resources	19	Low
Reliance on DNS Lookups in a Decision	16	Low
Improper Resource Access Authorization	11	Low
Use of Sizeof On a Pointer Type	3	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	39
chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	37
chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	37
chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	37
chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	37
chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	37
chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	37
chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	37
Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	28
Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c	28

Scan Results Details

Buffer Overflow Indexes

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

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=1
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in buf, at line 1714 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1939 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1939	1743
Object	argv	buf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
1939.  int main(int argc, char **argv) {
```

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1743.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&

	pathid=2
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in sizeof, at line 1714 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1939 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1939	1743
Object	argv	sizeof

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
1939.   int main(int argc, char **argv) {
```

▼

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1743.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=3
Status	New

The size of the buffer used by xmlNanoFTPList in buf, at line 1613 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1939 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1939	1640
Object	argv	buf

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
1939.  int main(int argc, char **argv) {
```

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1640.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=4
Status	New

The size of the buffer used by xmlNanoFTPList in sizeof, at line 1613 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1939 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1939	1640
Object	argv	sizeof

Code Snippet

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method int main(int argc, char **argv) {

```
....
1939.  int main(int argc, char **argv) {
```

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1640.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=5

Status	New

The size of the buffer used by xmlNanoFTPGetSocket in buf, at line 1835 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	buf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=6
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in sizeof, at line 1835 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	sizeof

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c

Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=7
Status	New

The size of the buffer used by xmlNanoFTPList in buf, at line 1725 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	buf

Code Snippet

File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c

Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c

Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=8

Status	New

The size of the buffer used by xmlNanoFTPList in sizeof, at line 1725 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	sizeof

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=9
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in buf, at line 1835 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	buf

Code Snippet

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name   chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c

Method   xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=10
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in sizeof, at line 1835 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	sizeof

Code Snippet

File Name   chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c

Method   int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name   chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c

Method   xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=11

Status	New

The size of the buffer used by xmlNanoFTPList in buf, at line 1725 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	buf

Code Snippet

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=12
Status	New

The size of the buffer used by xmlNanoFTPList in sizeof, at line 1725 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	sizeof

Code Snippet

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2072.   int main(int argc, char **argv) {
```

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=13
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in buf, at line 1835 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	buf

Code Snippet

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2072.   int main(int argc, char **argv) {
```

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=14

Status	New

The size of the buffer used by xmlNanoFTPGetSocket in sizeof, at line 1835 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

▼

File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=15
Status	New

The size of the buffer used by xmlNanoFTPList in buf, at line 1725 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	buf

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=16
Status	New

The size of the buffer used by xmlNanoFTPList in sizeof, at line 1725 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	sizeof

Code Snippet

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=17

Status	New

The size of the buffer used by xmlNanoFTPGetSocket in buf, at line 1835 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	buf

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

▼

File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=18
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in sizeof, at line 1835 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=19
Status	New

The size of the buffer used by xmlNanoFTPList in buf, at line 1725 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	buf

Code Snippet

File Name	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=20

Status	New

The size of the buffer used by xmlNanoFTPList in sizeof, at line 1725 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=21
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in buf, at line 1835 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	buf

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=22
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in sizeof, at line 1835 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	sizeof

Code Snippet

File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=23

Status	New

The size of the buffer used by xmlNanoFTPList in buf, at line 1725 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	buf

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

▼

File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=24
Status	New

The size of the buffer used by xmlNanoFTPList in sizeof, at line 1725 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	sizeof

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=25
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in buf, at line 1835 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	buf

Code Snippet

File Name	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=26

Status	New

The size of the buffer used by xmlNanoFTPGetSocket in sizeof, at line 1835 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	sizeof

Code Snippet

File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c

Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c

Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=27
Status	New

The size of the buffer used by xmlNanoFTPList in buf, at line 1725 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	buf

Code Snippet

File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c

Method int main(int argc, char **argv) {

```
....
2072.   int main(int argc, char **argv) {
```

File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c

Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=28
Status	New

The size of the buffer used by xmlNanoFTPList in sizeof, at line 1725 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	sizeof

Code Snippet

File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c

Method int main(int argc, char **argv) {

```
....
2072.   int main(int argc, char **argv) {
```

File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c

Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=29

Status	New

The size of the buffer used by xmlNanoFTPGetSocket in buf, at line 1835 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	buf

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.   int main(int argc, char **argv) {
```

File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c

Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=30
Status	New

The size of the buffer used by xmlNanoFTPGetSocket in sizeof, at line 1835 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	2072	1867
Object	argv	sizeof

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

▼

File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c

Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1867.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=31
Status	New

The size of the buffer used by xmlNanoFTPList in buf, at line 1725 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	buf

Code Snippet

File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c

Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

▼

File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c

Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=32

Status	New

The size of the buffer used by xmlNanoFTPList in sizeof, at line 1725 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 2072 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	2072	1752
Object	argv	sizeof

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2072.  int main(int argc, char **argv) {
```

▼

File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=33
Status	New

The size of the buffer used by xmlNanoFTPConnect in buf, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 154 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	181	944
Object	getenv	buf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPInit(void) {

```
....
181.       env = getenv("ftp_proxy_user");
```

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
944.                buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=34
Status	New

The size of the buffer used by xmlNanoFTPConnect in sizeof, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 154 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	181	944
Object	getenv	sizeof

Code Snippet

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPInit(void) {

```
....
181.       env = getenv("ftp_proxy_user");
```

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
944.                buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=35

Status	New

The size of the buffer used by xmlNanoFTPConnect in buf, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 154 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	185	964
Object	getenv	buf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPInit(void) {

```
....
185.        env = getenv("ftp_proxy_password");
```

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
964.                            buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=36
Status	New

The size of the buffer used by xmlNanoFTPConnect in sizeof, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 154 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	185	964
Object	getenv	sizeof

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPInit(void) {

```
....
185.        env = getenv("ftp_proxy_password");
```

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
964.                            buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=37
Status	New

The size of the buffer used by xmlNanoFTPConnect in buf, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	207	1022
Object	getenv	buf

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPInit(void) {

```
....
207.        env = getenv("ftp_proxy_user");
```

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
1022.                   buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=38

Status	New

The size of the buffer used by xmlNanoFTPConnect in sizeof, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	207	1022
Object	getenv	sizeof

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPInit(void) {

```
....
207.        env = getenv("ftp_proxy_user");
```

File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
1022.                buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=39
Status	New

The size of the buffer used by xmlNanoFTPConnect in buf, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	211	1045
Object	getenv	buf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPInit(void) {

```
....
211.       env = getenv("ftp_proxy_password");
```

▼

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
1045.                          buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=40
Status	New

The size of the buffer used by xmlNanoFTPConnect in sizeof, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	211	1045
Object	getenv	sizeof

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPInit(void) {

```
....
211.       env = getenv("ftp_proxy_password");
```

▼

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
1045.                          buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=41

Status	New

The size of the buffer used by xmlNanoFTPConnect in buf, at line 849 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	207	1022
Object	getenv	buf

Code Snippet

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	xmlNanoFTPInit(void) {

```
....
207.        env = getenv("ftp_proxy_user");
```

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
1022.               buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=42
Status	New

The size of the buffer used by xmlNanoFTPConnect in sizeof, at line 849 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	207	1022
Object	getenv	sizeof

Code Snippet

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	xmlNanoFTPInit(void) {

```
....
207.        env = getenv("ftp_proxy_user");
```

File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
1022.                   buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=43
Status	New

The size of the buffer used by xmlNanoFTPConnect in buf, at line 849 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	211	1045
Object	getenv	buf

Code Snippet

File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c

Method xmlNanoFTPInit(void) {

```
....
211.        env = getenv("ftp_proxy_password");
```

File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
1045.                           buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=44

Status	New

The size of the buffer used by xmlNanoFTPConnect in sizeof, at line 849 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	211	1045
Object	getenv	sizeof

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPInit(void) {

```
....
211.      env = getenv("ftp_proxy_password");
```

File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
1045.                       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=45
Status	New

The size of the buffer used by xmlNanoFTPConnect in buf, at line 849 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	207	1022
Object	getenv	buf

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPInit(void) {

```
....
207.      env = getenv("ftp_proxy_user");
```

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
1022.                buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=46
Status	New

The size of the buffer used by xmlNanoFTPConnect in sizeof, at line 849 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	207	1022
Object	getenv	sizeof

Code Snippet

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPInit(void) {

```
....
207.      env = getenv("ftp_proxy_user");
```

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
1022.                buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=47

Status	New

The size of the buffer used by xmlNanoFTPConnect in buf, at line 849 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	211	1045
Object	getenv	buf

Code Snippet

File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c

Method xmlNanoFTPInit(void) {

```
....
211.       env = getenv("ftp_proxy_password");
```

▼

File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
1045.                      buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=48
Status	New

The size of the buffer used by xmlNanoFTPConnect in sizeof, at line 849 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	211	1045
Object	getenv	sizeof

Code Snippet

File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c

Method xmlNanoFTPInit(void) {

```
....
211.        env = getenv("ftp_proxy_password");
```

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
1045.                       buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=49
Status	New

The size of the buffer used by xmlNanoFTPConnect in buf, at line 849 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	207	1022
Object	getenv	buf

Code Snippet

File Name	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method	xmlNanoFTPInit(void) {

```
....
207.        env = getenv("ftp_proxy_user");
```

File Name	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
1022.                 buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow Indexes\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=50

Status	New

The size of the buffer used by xmlNanoFTPConnect in sizeof, at line 849 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPInit passes to getenv, at line 180 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	207	1022
Object	getenv	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPInit(void) {

```
....
207.        env = getenv("ftp_proxy_user");
```

File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
1022.               buf[sizeof(buf) - 1] = 0;
```

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=67
Status	New

The size of the buffer used by Instance_DidCreate in i, at line 86 of chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Instance_DidCreate passes to getenv, at line 86 of chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c

Line	127	147
Object	getenv	i

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
127.        const char* next_arg = getenv(arg_name);
....
147.        PSInstanceTrace("argv[%d] '%s'\n", i, si->argv_[i]);
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=68
Status	New

The size of the buffer used by Instance_DidCreate in i, at line 86 of chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Instance_DidCreate passes to getenv, at line 86 of chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	127	147
Object	getenv	i

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
127.        const char* next_arg = getenv(arg_name);
....
147.        PSInstanceTrace("argv[%d] '%s'\n", i, si->argv_[i]);
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=69
Status	New

The size of the buffer used by Instance_DidCreate in i, at line 86 of chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Instance_DidCreate passes to getenv, at line 86 of chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	127	147
Object	getenv	i

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
127.        const char* next_arg = getenv(arg_name);
....
147.        PSInstanceTrace("argv[%d] '%s'\n", i, si->argv_[i]);
```

Buffer Overflow boundedcpy

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

Categories

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

Description

Buffer Overflow boundedcpy\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=65
Status	New

The size parameter h_length in line 771 in file chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c is influenced by the user input getenv in line 154 in file chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	172	867
Object	getenv	h_length

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPInit(void) {

```
....
172.        env = getenv("ftp_proxy");
```

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
867.                hp->h_addr_list[0], hp->h_length);
```

Buffer Overflow boundedcpy\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=66
Status	New

The size parameter h_length in line 771 in file chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c is influenced by the user input getenv in line 154 in file chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	176	867
Object	getenv	h_length

Code Snippet

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPInit(void) {

```
....
176.        env = getenv("FTP_PROXY");
```

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
867.                hp->h_addr_list[0], hp->h_length);
```

Dangerous Functions

Query Path:

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

Categories

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

Description

Dangerous Functions\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=567
Status	New

The dangerous function, alloca, was found in use at line 240 in chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	244	244
Object	alloca	alloca

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
244.    char* message = alloca(tty_prefix_len + count + 1);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=568
Status	New

The dangerous function, alloca, was found in use at line 361 in chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	369	369
Object	alloca	alloca

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method void ExitHandshake(int status, void* user_data) {

```
....
369.     char* message = alloca(message_len);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=569
Status	New

The dangerous function, alloca, was found in use at line 240 in chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	244	244
Object	alloca	alloca

Code Snippet

File Name	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method	ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
244.     char* message = alloca(tty_prefix_len + count + 1);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=570
Status	New

The dangerous function, alloca, was found in use at line 361 in chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	369	369
Object	alloca	alloca

Code Snippet

File Name	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c

Method void ExitHandshake(int status, void* user_data) {

```
....
369.    char* message = alloca(message_len);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=571
Status	New

The dangerous function, alloca, was found in use at line 240 in chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	244	244
Object	alloca	alloca

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
244.    char* message = alloca(tty_prefix_len + count + 1);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=572
Status	New

The dangerous function, alloca, was found in use at line 361 in chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	369	369
Object	alloca	alloca

Code Snippet

File Name	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method	void ExitHandshake(int status, void* user_data) {

```
....
369.     char* message = alloca(message_len);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=573
Status	New

The dangerous function, memcpy, was found in use at line 771 in chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	833	833
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
833.             memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=574
Status	New

The dangerous function, memcpy, was found in use at line 771 in chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	838	838
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
838.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=575
Status	New

The dangerous function, memcpy, was found in use at line 771 in chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	866	866
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
866.        memcpy (&((struct sockaddr_in *)&ctxt->ftpAddr)->sin_addr,
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=576
Status	New

The dangerous function, memcpy, was found in use at line 1274 in chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1348	1348
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1348.           memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=577
Status	New

The dangerous function, memcpy, was found in use at line 1274 in chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1364	1364
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1364.           memcpy (&((struct sockaddr_in *)&dataAddr)->sin_addr,
&ad[0], 4);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=578
Status	New

The dangerous function, memcpy, was found in use at line 1274 in chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Line	1365	1365
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1365.          memcpy (&((struct sockaddr_in *)&dataAddr)->sin_port,
&ad[4], 2);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=579
Status	New

The dangerous function, memcpy, was found in use at line 240 in chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	245	245
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
245.    memcpy(message, s_tty_prefix, tty_prefix_len);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=580
Status	New

The dangerous function, memcpy, was found in use at line 240 in chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	246	246
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
246.     memcpy(message + tty_prefix_len, data, count);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=581
Status	New

The dangerous function, memcpy, was found in use at line 240 in chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	245	245
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
245.     memcpy(message, s_tty_prefix, tty_prefix_len);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=582
Status	New

The dangerous function, memcpy, was found in use at line 240 in chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	246	246
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
246.     memcpy(message + tty_prefix_len, data, count);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=583
Status	New

The dangerous function, memcpy, was found in use at line 240 in chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	245	245
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
245.     memcpy(message, s_tty_prefix, tty_prefix_len);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=584
Status	New

The dangerous function, memcpy, was found in use at line 240 in chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	246	246
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
246.     memcpy(message + tty_prefix_len, data, count);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=585
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	911	911
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
911.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=586
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	916	916
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
916.              memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=587
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	944	944
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
944.          memcpy (&((struct sockaddr_in *)&ctxt->ftpAddr)->sin_addr,
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=588
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1450	1450
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.           memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=589
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1466	1466
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1466.           memcpy (&((struct sockaddr_in *)&dataAddr)->sin_addr,
&ad[0], 4);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=590
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1467	1467
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1467.           memcpy (&((struct sockaddr_in *)&dataAddr)->sin_port,
&ad[4], 2);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=591
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	911	911
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
911.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=592

Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	916	916
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
916.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=593
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	944	944
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
944.        memcpy (&((struct sockaddr_in *)&ctxt->ftpAddr)->sin_addr,
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&

	pathid=594
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1450	1450
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.           memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=595
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1466	1466
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1466.           memcpy (&((struct sockaddr_in *)&dataAddr)->sin_addr,
&ad[0], 4);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=596
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1467	1467
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetConnection(void *ctx) {

```
....
1467.         memcpy (&((struct sockaddr_in *)&dataAddr)->sin_port,
&ad[4], 2);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=597
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	911	911
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
911.          memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=598
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	916	916
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
916.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=599
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	944	944
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
944.        memcpy (&((struct sockaddr_in *)&ctxt->ftpAddr)->sin_addr,
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=600
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	1450	1450
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.           memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=601
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	1466	1466
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1466.           memcpy (&((struct sockaddr_in *)&dataAddr)->sin_addr,
&ad[0], 4);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=602
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	1467	1467
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1467.           memcpy (&((struct sockaddr_in *)&dataAddr)->sin_port,
&ad[4], 2);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=603
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	911	911

Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
911.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=604
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	916	916
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
916.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=605
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c

Line	944	944
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
944.        memcpy (&((struct sockaddr_in *)&ctxt->ftpAddr)->sin_addr,
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=606
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1450	1450
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.            memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=607
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1466	1466
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1466.         memcpy (&((struct sockaddr_in *)&dataAddr)->sin_addr,
&ad[0], 4);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=608
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1467	1467
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1467.         memcpy (&((struct sockaddr_in *)&dataAddr)->sin_port,
&ad[4], 2);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=609
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	911	911
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
911.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=610
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	916	916
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
916.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=611
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	944	944
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
944.        memcpy (&((struct sockaddr_in *)&ctxt->ftpAddr)->sin_addr,
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=612
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1450	1450
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.           memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=613
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1466	1466
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1466.          memcpy (&((struct sockaddr_in *)&dataAddr)->sin_addr,
&ad[0], 4);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=614
Status	New

The dangerous function, memcpy, was found in use at line 1373 in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1467	1467
Object	memcpy	memcpy

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1467.          memcpy (&((struct sockaddr_in *)&dataAddr)->sin_port,
&ad[4], 2);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&

	pathid=615
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	911	911
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
911.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=616
Status	New

The dangerous function, memcpy, was found in use at line 849 in chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	916	916
Object	memcpy	memcpy

Code Snippet

File Name	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
916.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

MemoryFree on StackVariable

Query Path:
CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0
Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=362
Status	New

Calling free() (line 322) on a variable that was not dynamically allocated (line 322) in file chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c may result with a crash.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	348	348
Object	si	si

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method void* MainThread(void* info) {

```
....
348.     free(si);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=363
Status	New

Calling free() (line 322) on a variable that was not dynamically allocated (line 322) in file chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c may result with a crash.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	348	348
Object	si	si

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method void* MainThread(void* info) {

```
....
348.     free(si);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=364
Status	New

Calling free() (line 322) on a variable that was not dynamically allocated (line 322) in file chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c may result with a crash.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	348	348
Object	si	si

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method void* MainThread(void* info) {

```
....
348.     free(si);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=365
Status	New

Calling free() (line 714) on a variable that was not dynamically allocated (line 714) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Line	794	794
Object	targetdir	targetdir

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Method int cli_scanhfsplus(cli_ctx *ctx)

```
....
794.         free(targetdir);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=366
Status	New

Calling free() (line 714) on a variable that was not dynamically allocated (line 714) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Line	796	796
Object	volHeader	volHeader

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Method	int cli_scanhfsplus(cli_ctx *ctx)

```
....
796.        free(volHeader);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=367
Status	New

Calling free() (line 289) on a variable that was not dynamically allocated (line 289) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Line	415	415
Object	tmpname	tmpname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Method	static int hfsplus_scanfile(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *extHeader,

```
....
415.        free(tmpname);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=368
Status	New

Calling free() (line 536) on a variable that was not dynamically allocated (line 536) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Line	706	706
Object	nodeBuf	nodeBuf

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Method	static int hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
706.        free(nodeBuf);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=369
Status	New

Calling free() (line 1095) on a variable that was not dynamically allocated (line 1095) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	1121	1121
Object	xmlfile	xmlfile

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method	static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1121.           free(xmlfile);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=370
Status	New

Calling free() (line 1095) on a variable that was not dynamically allocated (line 1095) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	1128	1128
Object	xmlfile	xmlfile

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1128.            free(xmlfile);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=371
Status	New

Calling free() (line 1095) on a variable that was not dynamically allocated (line 1095) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	1133	1133
Object	xmlfile	xmlfile

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1133.        free(xmlfile);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=372
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	164	164
Object	dirname	dirname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
164.              free(dirname);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=373
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	176	176
Object	dirname	dirname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
176.                  free(dirname);
```

MemoryFree on StackVariable\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=374
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	187	187
Object	dirname	dirname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
187.            free(dirname);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=375
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	197	197
Object	dirname	dirname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
197.            free(dirname);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&

	pathid=376
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	217	217
Object	dirname	dirname

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
217.            free(dirname);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=377
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	294	294
Object	mish_set	mish_set

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
294.                        free(mish_set);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=378

Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	299	299
Object	mish_set	mish_set

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
299.                            free(mish_set);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=379
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	451	451
Object	mish_list_tail	mish_list_tail

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
451.            free(mish_list_tail);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=380
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	460	460
Object	mish_list_tail	mish_list_tail

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
460.            free(mish_list_tail);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=381
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	464	464
Object	dirname	dirname

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
464.        free(dirname);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=382
Status	New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	494	494
Object	decoded	decoded

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
494.            free(decoded);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=383
Status	New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	501	501
Object	decoded	decoded

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
501.            free(decoded);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=384
Status	New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	509	509
Object	decoded	decoded

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
509.            free(decoded);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=385
Status	New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	528	528
Object	decoded	decoded

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
528.            free(decoded);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=386

Status	New

Calling free() (line 1423) on a variable that was not dynamically allocated (line 1423) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1515	1515
Object	targetdir	targetdir

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1515.       free(targetdir);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=387
Status	New

Calling free() (line 1423) on a variable that was not dynamically allocated (line 1423) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1517	1517
Object	volHeader	volHeader

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1517.       free(volHeader);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=388
Status	New

Calling free() (line 317) on a variable that was not dynamically allocated (line 317) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	444	444
Object	tmpname	tmpname

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_scanfile(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *extHeader,

```
....
444.            free(tmpname);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=389
Status	New

Calling free() (line 479) on a variable that was not dynamically allocated (line 479) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	624	624
Object	nodeBuf	nodeBuf

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_check_attribute(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *attrHeader, uint32_t expectedCnid, const uint8_t name[], uint32_t nameLen, int *found, uint8_t record[], unsigned *recordSize)

```
....
624.            free(nodeBuf);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&

	pathid=390
Status	New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	988	988
Object	name_utf8	name_utf8

Code Snippet	
File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method	static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
988.                            free(name_utf8);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=391
Status	New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1065	1065
Object	tmpname	tmpname

Code Snippet	
File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method	static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1065.                                           free(tmpname);
```

MemoryFree on StackVariable\Path 31:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=392
Status	New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1166	1166
Object	resourceFile	resourceFile

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method	static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1166.                                                   free(resourceFile);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=393
Status	New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1294	1294
Object	table	table

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method	static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1294.                                                            free(table);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=394
Status	New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1306	1306
Object	resourceFile	resourceFile

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method	static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1306.                                           free(resourceFile);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=395
Status	New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1340	1340
Object	tmpname	tmpname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method	static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1340.                                       free(tmpname);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=396
Status	New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1391	1391
Object	name_utf8	name_utf8

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method	static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1391.                       free(name_utf8);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=397
Status	New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1411	1411
Object	nodeBuf	nodeBuf

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method	static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1411.       free(nodeBuf);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=398
Status	New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1413	1413
Object	name_utf8	name_utf8

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method	static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1413.           free(name_utf8);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=399
Status	New

Calling free() (line 1096) on a variable that was not dynamically allocated (line 1096) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	1122	1122
Object	xmlfile	xmlfile

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method	static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1122.           free(xmlfile);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=400
Status	New

Calling free() (line 1096) on a variable that was not dynamically allocated (line 1096) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	1129	1129
Object	xmlfile	xmlfile

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1129.           free(xmlfile);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=401
Status	New

Calling free() (line 1096) on a variable that was not dynamically allocated (line 1096) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	1134	1134
Object	xmlfile	xmlfile

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1134.       free(xmlfile);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=402
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	164	164
Object	dirname	dirname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
164.            free(dirname);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=403
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	176	176
Object	dirname	dirname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
176.                free(dirname);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=404
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	187	187
Object	dirname	dirname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
187.            free(dirname);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=405
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	197	197
Object	dirname	dirname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
197.            free(dirname);
```

MemoryFree on StackVariable\Path 45:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=406
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	217	217
Object	dirname	dirname

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
217.            free(dirname);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=407
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	294	294
Object	mish_set	mish_set

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
294.                            free(mish_set);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&

	pathid=408
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	299	299
Object	mish_set	mish_set

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
299.                            free(mish_set);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=409
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	451	451
Object	mish_list_tail	mish_list_tail

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
451.            free(mish_list_tail);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=410

Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	460	460
Object	mish_list_tail	mish_list_tail

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
460.            free(mish_list_tail);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=411
Status	New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c may result with a crash.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	464	464
Object	dirname	dirname

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
464.        free(dirname);
```

Buffer Overflow boundcpy WrongSizeParam

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

Categories

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

Description

Buffer Overflow boundcpy WrongSizeParam\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=285
Status	New

The size of the buffer used by xmlNanoFTPGetConnection in in6_addr, at line 1274 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPGetConnection passes to in6_addr, at line 1274 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1348	1348
Object	in6_addr	in6_addr

Code Snippet

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1348.               memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=286
Status	New

The size of the buffer used by xmlNanoFTPGetConnection in in6_addr, at line 1373 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPGetConnection passes to in6_addr, at line 1373 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1450	1450
Object	in6_addr	in6_addr

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.            memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=287
Status	New

The size of the buffer used by xmlNanoFTPGetConnection in in6_addr, at line 1373 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPGetConnection passes to in6_addr, at line 1373 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1450	1450
Object	in6_addr	in6_addr

Code Snippet

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.            memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=288
Status	New

The size of the buffer used by xmlNanoFTPGetConnection in in6_addr, at line 1373 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPGetConnection passes to in6_addr, at line 1373 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-	chromium@@chromium-88.0.4287.1-

	CVE-2021-3520-FP.c	CVE-2021-3520-FP.c
Line	1450	1450
Object	in6_addr	in6_addr

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.             memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=289
Status	New

The size of the buffer used by xmlNanoFTPGetConnection in in6_addr, at line 1373 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPGetConnection passes to in6_addr, at line 1373 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1450	1450
Object	in6_addr	in6_addr

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.             memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=290
Status	New

The size of the buffer used by xmlNanoFTPGetConnection in in6_addr, at line 1373 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPGetConnection passes to in6_addr, at line 1373 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1450	1450
Object	in6_addr	in6_addr

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.            memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=291
Status	New

The size of the buffer used by xmlNanoFTPGetConnection in in6_addr, at line 1373 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPGetConnection passes to in6_addr, at line 1373 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	1450	1450
Object	in6_addr	in6_addr

Code Snippet
File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.            memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=292
Status	New

The size of the buffer used by xmlNanoFTPGetConnection in in6_addr, at line 1373 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPGetConnection passes to in6_addr, at line 1373 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	1450	1450
Object	in6_addr	in6_addr

Code Snippet	
File Name	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetConnection(void *ctx) {

```
....
1450.            memcpy (&((struct sockaddr_in6 *)&dataAddr)->sin6_addr,
&((struct sockaddr_in6 *)&ctxt->ftpAddr)->sin6_addr, sizeof(struct
in6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=293
Status	New

The size of the buffer used by hfsplus_readheader in hfsNodeDescriptor, at line 200 of Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsNodeDescriptor, at line 200 of Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Line	242	242
Object	hfsNodeDescriptor	hfsNodeDescriptor

Code Snippet	
File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Method	static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
242.        memcpy(nodeDesc, mPtr, sizeof(hfsNodeDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=294
Status	New

The size of the buffer used by hfsplus_readheader in hfsHeaderRecord, at line 200 of Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsHeaderRecord, at line 200 of Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Line	255	255
Object	hfsHeaderRecord	hfsHeaderRecord

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Method	static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
255.        memcpy(headerRec, mPtr + sizeof(hfsNodeDescriptor),
sizeof(hfsHeaderRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=295
Status	New

The size of the buffer used by hfsplus_walk_catalog in hfsPlusCatalogFile, at line 536 of Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_walk_catalog passes to hfsPlusCatalogFile, at line 536 of Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Line	643	643
Object	hfsPlusCatalogFile	hfsPlusCatalogFile

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Method static int hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
643.                memcpy(&fileRec, &(nodeBuf[recordStart + keylen + 2]),
sizeof(hfsPlusCatalogFile));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=296
Status	New

The size of the buffer used by hfsplus_readheader in hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	254	254
Object	hfsNodeDescriptor	hfsNodeDescriptor

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
254.        memcpy(nodeDesc, mPtr, sizeof(hfsNodeDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=297
Status	New

The size of the buffer used by hfsplus_readheader in hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination

File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	267	267
Object	hfsHeaderRecord	hfsHeaderRecord

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
267.      memcpy(headerRec, mPtr + sizeof(hfsNodeDescriptor),
sizeof(hfsHeaderRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=298
Status	New

The size of the buffer used by hfsplus_walk_catalog in hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_walk_catalog passes to hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	999	999
Object	hfsPlusCatalogFile	hfsPlusCatalogFile

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
999.            memcpy(&fileRec, &(nodeBuf[recordStart + keylen + 2]),
sizeof(hfsPlusCatalogFile));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=299
Status	New

The size of the buffer used by hfsplus_readheader in hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c
Line	254	254
Object	hfsNodeDescriptor	hfsNodeDescriptor

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
254.       memcpy(nodeDesc, mPtr, sizeof(hfsNodeDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=300
Status	New

The size of the buffer used by hfsplus_readheader in hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c
Line	267	267
Object	hfsHeaderRecord	hfsHeaderRecord

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
267.       memcpy(headerRec, mPtr + sizeof(hfsNodeDescriptor),
sizeof(hfsHeaderRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=301
Status	New

The size of the buffer used by hfsplus_walk_catalog in hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_walk_catalog passes to hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c
Line	999	999
Object	hfsPlusCatalogFile	hfsPlusCatalogFile

Code Snippet

File Name Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c

Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
999.                memcpy(&fileRec, &(nodeBuf[recordStart + keylen + 2]),
sizeof(hfsPlusCatalogFile));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=302
Status	New

The size of the buffer used by hfsplus_readheader in hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c
Line	254	254
Object	hfsNodeDescriptor	hfsNodeDescriptor

Code Snippet

File Name Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c

Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
254.       memcpy(nodeDesc, mPtr, sizeof(hfsNodeDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=303
Status	New

The size of the buffer used by hfsplus_readheader in hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c
Line	267	267
Object	hfsHeaderRecord	hfsHeaderRecord

Code Snippet

File Name   Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c

Method   static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
267.       memcpy(headerRec, mPtr + sizeof(hfsNodeDescriptor),
sizeof(hfsHeaderRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=304
Status	New

The size of the buffer used by hfsplus_walk_catalog in hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_walk_catalog passes to hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c
Line	999	999
Object	hfsPlusCatalogFile	hfsPlusCatalogFile

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c
Method	static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
999.                memcpy(&fileRec, &(nodeBuf[recordStart + keylen + 2]),
sizeof(hfsPlusCatalogFile));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=305
Status	New

The size of the buffer used by hfsplus_readheader in hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c
Line	254	254
Object	hfsNodeDescriptor	hfsNodeDescriptor

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c
Method	static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
254.        memcpy(nodeDesc, mPtr, sizeof(hfsNodeDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=306
Status	New

The size of the buffer used by hfsplus_readheader in hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination

File	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c
Line	267	267
Object	hfsHeaderRecord	hfsHeaderRecord

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
267.       memcpy(headerRec, mPtr + sizeof(hfsNodeDescriptor),
sizeof(hfsHeaderRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=307
Status	New

The size of the buffer used by hfsplus_walk_catalog in hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_walk_catalog passes to hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c
Line	999	999
Object	hfsPlusCatalogFile	hfsPlusCatalogFile

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
999.             memcpy(&fileRec, &(nodeBuf[recordStart + keylen + 2]),
sizeof(hfsPlusCatalogFile));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=308
Status	New

The size of the buffer used by hfsplus_readheader in hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c
Line	254	254
Object	hfsNodeDescriptor	hfsNodeDescriptor

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
254.        memcpy(nodeDesc, mPtr, sizeof(hfsNodeDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=309
Status	New

The size of the buffer used by hfsplus_readheader in hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c
Line	267	267
Object	hfsHeaderRecord	hfsHeaderRecord

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
267.        memcpy(headerRec, mPtr + sizeof(hfsNodeDescriptor),
sizeof(hfsHeaderRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=310
Status	New

The size of the buffer used by hfsplus_walk_catalog in hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_walk_catalog passes to hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c, to overwrite the target buffer.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c
Line	999	999
Object	hfsPlusCatalogFile	hfsPlusCatalogFile

Code Snippet

File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c

Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
999.                memcpy(&fileRec, &(nodeBuf[recordStart + keylen + 2]),
sizeof(hfsPlusCatalogFile));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=311
Status	New

The size of the buffer used by xmlNanoFTPNewCtxt in xmlNanoFTPCtxt, at line 430 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPNewCtxt passes to xmlNanoFTPCtxt, at line 430 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	440	440
Object	xmlNanoFTPCtxt	xmlNanoFTPCtxt

Code Snippet

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPNewCtxt(const char *URL) {

```
....
440.       memset(ret, 0, sizeof(xmlNanoFTPCtxt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=312
Status	New

The size of the buffer used by xmlNanoFTPConnect in ->, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to ->, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	794	794
Object	->	->

Code Snippet
File Name   chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method   xmlNanoFTPConnect(void *ctx) {

```
....
794.       memset (&ctxt->ftpAddr, 0, sizeof(ctxt->ftpAddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=313
Status	New

The size of the buffer used by xmlNanoFTPNewCtxt in xmlNanoFTPCtxt, at line 464 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPNewCtxt passes to xmlNanoFTPCtxt, at line 464 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	474	474
Object	xmlNanoFTPCtxt	xmlNanoFTPCtxt

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPNewCtxt(const char *URL) {

```
....
474.        memset(ret, 0, sizeof(xmlNanoFTPCtxt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=314
Status	New

The size of the buffer used by xmlNanoFTPConnect in ->, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to ->, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	872	872
Object	->	->

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
872.        memset (&ctxt->ftpAddr, 0, sizeof(ctxt->ftpAddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=315
Status	New

The size of the buffer used by xmlNanoFTPNewCtxt in xmlNanoFTPCtxt, at line 464 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPNewCtxt passes to xmlNanoFTPCtxt, at line 464 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	474	474
Object	xmlNanoFTPCtxt	xmlNanoFTPCtxt

Code Snippet

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	xmlNanoFTPNewCtxt(const char *URL) {

```
....
474.      memset(ret, 0, sizeof(xmlNanoFTPCtxt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=316
Status	New

The size of the buffer used by xmlNanoFTPConnect in ->, at line 849 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to ->, at line 849 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	872	872
Object	->	->

Code Snippet

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
872.      memset (&ctxt->ftpAddr, 0, sizeof(ctxt->ftpAddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=317
Status	New

The size of the buffer used by xmlNanoFTPNewCtxt in xmlNanoFTPCtxt, at line 464 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPNewCtxt passes to xmlNanoFTPCtxt, at line 464 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c

Line	474	474
Object	xmlNanoFTPCtxt	xmlNanoFTPCtxt

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPNewCtxt(const char *URL) {

```
....
474.       memset(ret, 0, sizeof(xmlNanoFTPCtxt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=318
Status	New

The size of the buffer used by xmlNanoFTPConnect in ->, at line 849 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to ->, at line 849 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	872	872
Object	->	->

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
872.       memset (&ctxt->ftpAddr, 0, sizeof(ctxt->ftpAddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=319
Status	New

The size of the buffer used by xmlNanoFTPNewCtxt in xmlNanoFTPCtxt, at line 464 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPNewCtxt passes to xmlNanoFTPCtxt, at line 464 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination

File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	474	474
Object	xmlNanoFTPCtxt	xmlNanoFTPCtxt

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPNewCtxt(const char *URL) {

```
....
474.      memset(ret, 0, sizeof(xmlNanoFTPCtxt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=320
Status	New

The size of the buffer used by xmlNanoFTPConnect in ->, at line 849 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to ->, at line 849 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	872	872
Object	->	->

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
872.      memset (&ctxt->ftpAddr, 0, sizeof(ctxt->ftpAddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=321
Status	New

The size of the buffer used by xmlNanoFTPNewCtxt in xmlNanoFTPCtxt, at line 464 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPNewCtxt passes to xmlNanoFTPCtxt, at line 464 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	474	474
Object	xmlNanoFTPCtxt	xmlNanoFTPCtxt

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPNewCtxt(const char *URL) {

```
....
474.       memset(ret, 0, sizeof(xmlNanoFTPCtxt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=322
Status	New

The size of the buffer used by xmlNanoFTPConnect in ->, at line 849 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to ->, at line 849 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	872	872
Object	->	->

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
872.       memset (&ctxt->ftpAddr, 0, sizeof(ctxt->ftpAddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=323
Status	New

The size of the buffer used by xmlNanoFTPNewCtxt in xmlNanoFTPCtxt, at line 464 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPNewCtxt passes to xmlNanoFTPCtxt, at line 464 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	474	474
Object	xmlNanoFTPCtxt	xmlNanoFTPCtxt

Code Snippet
File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method xmlNanoFTPNewCtxt(const char *URL) {

```
....
474.       memset(ret, 0, sizeof(xmlNanoFTPCtxt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=324
Status	New

The size of the buffer used by xmlNanoFTPConnect in ->, at line 849 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to ->, at line 849 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	872	872
Object	->	->

Code Snippet
File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
872.       memset (&ctxt->ftpAddr, 0, sizeof(ctxt->ftpAddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=325

Status	New

The size of the buffer used by xmlNanoFTPNewCtxt in xmlNanoFTPCtxt, at line 464 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPNewCtxt passes to xmlNanoFTPCtxt, at line 464 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	474	474
Object	xmlNanoFTPCtxt	xmlNanoFTPCtxt

Code Snippet

File Name	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method	xmlNanoFTPNewCtxt(const char *URL) {

```
....
474.      memset(ret, 0, sizeof(xmlNanoFTPCtxt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=326
Status	New

The size of the buffer used by xmlNanoFTPConnect in ->, at line 849 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to ->, at line 849 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	872	872
Object	->	->

Code Snippet

File Name	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
872.      memset (&ctxt->ftpAddr, 0, sizeof(ctxt->ftpAddr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=327
Status	New

The size of the buffer used by xmlNanoFTPConnect in tmp, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to tmp, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	833	833
Object	tmp	tmp

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
833.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=328
Status	New

The size of the buffer used by xmlNanoFTPConnect in tmp, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to tmp, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	838	838
Object	tmp	tmp

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
838.            memcpy (&ctxt->ftpAddr, tmp->ai_addr, tmp->ai_addrlen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=329
Status	New

The size of the buffer used by xmlNanoFTPConnect in hp, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmlNanoFTPConnect passes to hp, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	867	867
Object	hp	hp

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
867.                hp->h_addr_list[0], hp->h_length);
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=330
Status	New

The size of the buffer used by TtyOutputHandler in tty_prefix_len, at line 240 of chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TtyOutputHandler passes to tty_prefix_len, at line 240 of chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	245	245
Object	tty_prefix_len	tty_prefix_len

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
245.     memcpy(message, s_tty_prefix, tty_prefix_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=331
Status	New

The size of the buffer used by TtyOutputHandler in count, at line 240 of chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TtyOutputHandler passes to count, at line 240 of chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	246	246
Object	count	count

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
246.    memcpy(message + tty_prefix_len, data, count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=332
Status	New

The size of the buffer used by TtyOutputHandler in tty_prefix_len, at line 240 of chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TtyOutputHandler passes to tty_prefix_len, at line 240 of chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	245	245
Object	tty_prefix_len	tty_prefix_len

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
245.    memcpy(message, s_tty_prefix, tty_prefix_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=333
Status	New

The size of the buffer used by TtyOutputHandler in count, at line 240 of chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TtyOutputHandler passes to count, at line 240 of chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	246	246
Object	count	count

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
246.    memcpy(message + tty_prefix_len, data, count);
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=334
Status	New

The size of the buffer used by TtyOutputHandler in tty_prefix_len, at line 240 of chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TtyOutputHandler passes to tty_prefix_len, at line 240 of chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	245	245
Object	tty_prefix_len	tty_prefix_len

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method ssize_t TtyOutputHandler(const char* data, size_t count, void* user_data) {

```
....
245.    memcpy(message, s_tty_prefix, tty_prefix_len);
```

Use of Zero Initialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Zero Initialized Pointer Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Zero Initialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=858
Status	New

The variable declared in next at Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c in line 95 is not initialized when it is used by next at Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c in line 95.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	310	304
Object	next	next

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
310.                      mish_list_tail->next = NULL;
....
304.                          mish_list_tail->next = mish_set;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=859
Status	New

The variable declared in next at Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c in line 95 is not initialized when it is used by mish_list at Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c in line 95.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	310	307

Object	next	mish_list

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
310.                    mish_list_tail->next = NULL;
....
307.                        mish_list       = mish_set;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=860
Status	New

The variable declared in next at Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c in line 95 is not initialized when it is used by next at Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c in line 95.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	310	304
Object	next	next

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
310.                    mish_list_tail->next = NULL;
....
304.                        mish_list_tail->next = mish_set;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=861
Status	New

The variable declared in next at Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c in line 95 is not initialized when it is used by mish_list at Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c in line 95.

	Source	Destination

File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	310	307
Object	next	mish_list

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
310.                  mish_list_tail->next = NULL;
....
307.                      mish_list      = mish_set;
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=862
Status	New

The variable declared in next at Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c in line 95 is not initialized when it is used by next at Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c in line 95.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c
Line	310	304
Object	next	next

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
310.                  mish_list_tail->next = NULL;
....
304.                      mish_list_tail->next = mish_set;
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=863
Status	New

The variable declared in next at Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c in line 95 is not initialized when it is used by mish_list at Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c in line 95.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c
Line	310	307
Object	next	mish_list

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
310.                    mish_list_tail->next = NULL;
....
307.                        mish_list      = mish_set;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=864
Status	New

The variable declared in next at Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c in line 95 is not initialized when it is used by next at Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c in line 95.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c
Line	310	304
Object	next	next

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
310.                    mish_list_tail->next = NULL;
....
304.                        mish_list_tail->next = mish_set;
```

Use of Zero Initialized Pointer\Path 8:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=865
Status	New

The variable declared in next at Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c in line 95 is not initialized when it is used by mish_list at Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c in line 95.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c
Line	310	307
Object	next	mish_list

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
310.                  mish_list_tail->next = NULL;
....
307.                      mish_list      = mish_set;
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=866
Status	New

The variable declared in next at Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c in line 95 is not initialized when it is used by next at Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c in line 95.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c
Line	310	304
Object	next	next

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c
Method	int cli_scandmg(cli_ctx *ctx)

```
....
310.                  mish_list_tail->next = NULL;
....
304.                      mish_list_tail->next = mish_set;
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=867
Status	New

The variable declared in next at Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c in line 95 is not initialized when it is used by mish_list at Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c in line 95.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c
Line	310	307
Object	next	mish_list

Code Snippet

File Name Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c

Method int cli_scandmg(cli_ctx *ctx)

```
....
310.                    mish_list_tail->next = NULL;
....
307.                        mish_list      = mish_set;
```

Memory Leak

Query Path:

CPP\Cx\CPP Medium Threat\Memory Leak Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Memory Leak\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=849
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	98	98
Object	si	si

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method	static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
98.     struct StartInfo* si = malloc(sizeof(struct StartInfo));
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=850
Status	New

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	98	98
Object	si	si

Code Snippet

File Name	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method	static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
98.     struct StartInfo* si = malloc(sizeof(struct StartInfo));
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=851
Status	New

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	98	98
Object	si	si

Code Snippet

File Name	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method	static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
98.     struct StartInfo* si = malloc(sizeof(struct StartInfo));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=852
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	101	101
Object	argv_	argv_

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
101.     si->argv_ = calloc(argc + 1, sizeof(char*));
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=853
Status	New

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	101	101
Object	argv_	argv_

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
101.     si->argv_ = calloc(argc + 1, sizeof(char*));
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=854
Status	New

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	101	101
Object	argv_	argv_

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
101.     si->argv_ = calloc(argc + 1, sizeof(char*));
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=855
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	131	131
Object	argv_	argv_

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
131.       si->argv_[si->argc_++] = strdup(next_arg);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=856
Status	New

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	131	131

Object	argv_	argv_

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
131.      si->argv_[si->argc_++] = strdup(next_arg);
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=857
Status	New

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	131	131
Object	argv_	argv_

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
131.      si->argv_[si->argc_++] = strdup(next_arg);
```

Buffer Overflow AddressOfLocalVarReturned

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=280
Status	New

The pointer b at Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c in line 541 is being used after it has been freed.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	544	544
Object	b	b

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Method	static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
544.        return a->startSector - b->startSector;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=281
Status	New

The pointer b at Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c in line 541 is being used after it has been freed.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	544	544
Object	b	b

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method	static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
544.        return a->startSector - b->startSector;
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=282
Status	New

The pointer b at Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c in line 541 is being used after it has been freed.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c
Line	544	544
Object	b	b

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c
Method	static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
544.        return a->startSector - b->startSector;
```

Buffer Overflow AddressOfLocalVarReturned\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=283
Status	New

The pointer b at Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c in line 541 is being used after it has been freed.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c
Line	544	544
Object	b	b

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c
Method	static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
544.        return a->startSector - b->startSector;
```

Buffer Overflow AddressOfLocalVarReturned\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=284
Status	New

The pointer b at Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c in line 541 is being used after it has been freed.

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c
Line	544	544
Object	b	b

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c
Method static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
544.       return a->startSector - b->startSector;
```

Environment Injection

Query Path:
CPP\Cx\CPP Medium Threat\Environment Injection Version:0

Categories

OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Environment Injection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=846
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	121	121
Object	getenv	setenv

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
121.     setenv("ARG0", getenv("SRC"), 0);
```

Environment Injection\Path 2:

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

	[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=847]()
Status	New

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	121	121
Object	getenv	setenv

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
121.     setenv("ARG0", getenv("SRC"), 0);
```

Environment Injection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	[http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=848]()
Status	New

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	121	121
Object	getenv	setenv

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
121.     setenv("ARG0", getenv("SRC"), 0);
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

NIST SP 800-53: SI-11 Error Handling (P2)

Description

Unchecked Return Value\Path 1:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=70
Status	New

The xmlNanoFTPSendUser method calls the snprintf function, at line 688 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	695	695
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPSendUser(void *ctx) {

```
....
695.         snprintf(buf, sizeof(buf), "USER anonymous\r\n");
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=71
Status	New

The xmlNanoFTPSendUser method calls the snprintf function, at line 688 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	697	697
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPSendUser(void *ctx) {

```
....
697.         snprintf(buf, sizeof(buf), "USER %s\r\n", ctxt->user);
```

Unchecked Return Value\Path 3:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=72
Status	New

The xmlNanoFTPSendPasswd method calls the snprintf function, at line 713 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	720	720
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPSendPasswd(void *ctx) {

```
....
720.         snprintf(buf, sizeof(buf), "PASS anonymous@\r\n");
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=73
Status	New

The xmlNanoFTPSendPasswd method calls the snprintf function, at line 713 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	722	722
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPSendPasswd(void *ctx) {

```
....
722.         snprintf(buf, sizeof(buf), "PASS %s\r\n", ctxt->passwd);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=74
Status	New

The xmlNanoFTPQuit method calls the snprintf function, at line 744 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	751	751
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPQuit(void *ctx) {

```
....
751.       snprintf(buf, sizeof(buf), "QUIT\r\n");
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=75
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	943	943
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
943.            snprintf(buf, sizeof(buf), "USER %s\r\n", proxyUser);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=76
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	961	961
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
961.                snprintf(buf, sizeof(buf), "PASS %s\r\n",
proxyPasswd);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=77
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	963	963
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
963.                    snprintf(buf, sizeof(buf), "PASS
anonymous@\r\n");
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=78
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1001	1001
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
1001.             snprintf(buf, sizeof(buf), "SITE %s\r\n", ctxt-
>hostname);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=79
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1026	1026
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
1026.             snprintf(buf, sizeof(buf), "USER
anonymous@%s\r\n",
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=80
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1029	1029
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
1029.             snprintf(buf, sizeof(buf), "USER %s@%s\r\n",
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=81
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1047	1047

Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
1047.              snprintf(buf, sizeof(buf), "PASS anonymous@\r\n");
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=82
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1049	1049
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
1049.              snprintf(buf, sizeof(buf), "PASS %s\r\n", ctxt-
>passwd);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=83
Status	New

The xmlNanoFTPCwd method calls the snprintf function, at line 1181 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Line	1197	1197
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPCwd(void *ctx, const char *directory) {

```
....
1197.       snprintf(buf, sizeof(buf), "CWD %s\r\n", directory);
```

Unchecked Return Value\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=84
Status New

The xmlNanoFTPDele method calls the snprintf function, at line 1227 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1245	1245
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPDele(void *ctx, const char *file) {

```
....
1245.       snprintf(buf, sizeof(buf), "DELE %s\r\n", file);
```

Unchecked Return Value\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=85
Status New

The xmlNanoFTPGetConnection method calls the snprintf function, at line 1274 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-	chromium@@chromium-

	120.0.6099.308-CVE-2021-3520-FP.c	120.0.6099.308-CVE-2021-3520-FP.c
Line	1312	1312
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1312.            snprintf (buf, sizeof(buf), "EPSV\r\n");
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=86
Status	New

The xmlNanoFTPGetConnection method calls the snprintf function, at line 1274 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1315	1315
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1315.            snprintf (buf, sizeof(buf), "PASV\r\n");
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=87
Status	New

The xmlNanoFTPGetConnection method calls the snprintf function, at line 1274 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1401	1401
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1401.           snprintf (buf, sizeof(buf), "EPRT |2|%s|%s|\r\n", adp,
portp);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=88
Status	New

The xmlNanoFTPGetConnection method calls the snprintf function, at line 1274 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1407	1407
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPGetConnection(void *ctx) {

```
....
1407.           snprintf (buf, sizeof(buf), "PORT
%d,%d,%d,%d,%d,%d\r\n",
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=89
Status	New

The xmlNanoFTPList method calls the snprintf function, at line 1613 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1629	1629
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1629.         snprintf(buf, sizeof(buf), "LIST -L\r\n");
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=90
Status	New

The xmlNanoFTPList method calls the snprintf function, at line 1613 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1638	1638
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1638.         snprintf(buf, sizeof(buf), "LIST -L %s\r\n", filename);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=91
Status	New

The xmlNanoFTPGetSocket method calls the snprintf function, at line 1714 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1726	1726
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1726.       snprintf(buf, sizeof(buf), "TYPE I\r\n");
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=92
Status	New

The xmlNanoFTPGetSocket method calls the snprintf function, at line 1714 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1740	1740
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1740.        snprintf(buf, sizeof(buf), "RETR %s\r\n", ctxt->path);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=93
Status	New

The xmlNanoFTPGetSocket method calls the snprintf function, at line 1714 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1742	1742
Object	snprintf	snprintf

Code Snippet

File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c

Method xmlNanoFTPGetSocket(void *ctx, const char *filename) {

```
....
1742.        snprintf(buf, sizeof(buf), "RETR %s\r\n", filename);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=94
Status	New

The Instance_DidCreate method calls the snprintf function, at line 86 of chromium@@chromium-120.0.6099.308-CVE-2021-44109-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	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	126	126
Object	snprintf	snprintf

Code Snippet

File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c

Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
126.      snprintf(arg_name, 32, "ARG%d", si->argc_);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=95
Status	New

The ExitHandshake method calls the snprintf function, at line 361 of chromium@@chromium-120.0.6099.308-CVE-2021-44109-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	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	370	370
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method void ExitHandshake(int status, void* user_data) {

```
....
370.     snprintf(message, message_len, "%s:%d", s_exit_message, status);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=96
Status	New

The Instance_DidCreate method calls the snprintf function, at line 86 of chromium@@chromium-122.0.6238.2-CVE-2021-44109-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	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	126	126
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
126.       snprintf(arg_name, 32, "ARG%d", si->argc_);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=97
Status	New

The ExitHandshake method calls the snprintf function, at line 361 of chromium@@chromium-122.0.6238.2-CVE-2021-44109-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	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	370	370
Object	snprintf	snprintf

Code Snippet
File Name	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method	void ExitHandshake(int status, void* user_data) {

```
....
370.     snprintf(message, message_len, "%s:%d", s_exit_message, status);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=98
Status	New

The Instance_DidCreate method calls the snprintf function, at line 86 of chromium@@chromium-127.0.6533.45-CVE-2021-44109-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	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	126	126
Object	snprintf	snprintf

Code Snippet
File Name	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method	static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
126.       snprintf(arg_name, 32, "ARG%d", si->argc_);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=99
Status	New

The ExitHandshake method calls the snprintf function, at line 361 of chromium@@chromium-127.0.6533.45-CVE-2021-44109-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	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	370	370
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method void ExitHandshake(int status, void* user_data) {

```
....
370.     snprintf(message, message_len, "%s:%d", s_exit_message, status);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=100
Status	New

The xmlNanoFTPSendUser method calls the snprintf function, at line 757 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	764	764
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPSendUser(void *ctx) {

```
....
764.         snprintf(buf, sizeof(buf), "USER anonymous\r\n");
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=101
Status	New

The xmlNanoFTPSendUser method calls the snprintf function, at line 757 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	766	766
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPSendUser(void *ctx) {

```
....
766.        snprintf(buf, sizeof(buf), "USER %s\r\n", ctxt->user);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=102
Status	New

The xmlNanoFTPSendPasswd method calls the snprintf function, at line 785 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	792	792
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPSendPasswd(void *ctx) {

```
....
792.        snprintf(buf, sizeof(buf), "PASS anonymous@\r\n");
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=103
Status	New

The xmlNanoFTPSendPasswd method calls the snprintf function, at line 785 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	794	794
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPSendPasswd(void *ctx) {

```
....
794.        snprintf(buf, sizeof(buf), "PASS %s\r\n", ctxt->passwd);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=104
Status	New

The xmlNanoFTPQuit method calls the snprintf function, at line 819 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	826	826
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPQuit(void *ctx) {

```
....
826.      snprintf(buf, sizeof(buf), "QUIT\r\n");
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=105
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1021	1021
Object	snprintf	snprintf

Code Snippet

File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
1021.           snprintf(buf, sizeof(buf), "USER %s\r\n", proxyUser);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=106
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1042	1042
Object	snprintf	snprintf

Code Snippet

File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c

Method xmlNanoFTPConnect(void *ctx) {

```
....
1042.                   snprintf(buf, sizeof(buf), "PASS %s\r\n",
proxyPasswd);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=107
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1044	1044
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
1044.                snprintf(buf, sizeof(buf), "PASS
anonymous@\r\n");
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=108
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1085	1085
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
1085.            snprintf(buf, sizeof(buf), "SITE %s\r\n", ctxt-
>hostname);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&

	pathid=109
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1113	1113
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
1113.                    snprintf(buf, sizeof(buf), "USER 
anonymous@%s\r\n",
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=110
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1116	1116
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
1116.                    snprintf(buf, sizeof(buf), "USER %s@%s\r\n",
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=111
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1137	1137
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
1137.               snprintf(buf, sizeof(buf), "PASS anonymous@\r\n");
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=112
Status	New

The xmlNanoFTPConnect method calls the snprintf function, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1139	1139
Object	snprintf	snprintf

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
1139.               snprintf(buf, sizeof(buf), "PASS %s\r\n", ctxt-
>passwd);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=113
Status	New

The xmlNanoFTPCwd method calls the snprintf function, at line 1274 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1290	1290
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPCwd(void *ctx, const char *directory) {

```
....
1290.       snprintf(buf, sizeof(buf), "CWD %s\r\n", directory);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=114
Status	New

The xmlNanoFTPDele method calls the snprintf function, at line 1323 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1341	1341
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPDele(void *ctx, const char *file) {

```
....
1341.       snprintf(buf, sizeof(buf), "DELE %s\r\n", file);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=115
Status	New

The xmlNanoFTPGetConnection method calls the snprintf function, at line 1373 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1411	1411
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetConnection(void *ctx) {

```
....
1411.            snprintf (buf, sizeof(buf), "EPSV\r\n");
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=116
Status	New

The xmlNanoFTPGetConnection method calls the snprintf function, at line 1373 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1414	1414
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetConnection(void *ctx) {

```
....
1414.            snprintf (buf, sizeof(buf), "PASV\r\n");
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=117
Status	New

The xmlNanoFTPGetConnection method calls the snprintf function, at line 1373 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1503	1503
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetConnection(void *ctx) {

```
....
1503.           snprintf (buf, sizeof(buf), "EPRT |2|%s|%s|\r\n", adp,
portp);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=118
Status	New

The xmlNanoFTPGetConnection method calls the snprintf function, at line 1373 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1509	1509
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPGetConnection(void *ctx) {

```
....
1509.            snprintf (buf, sizeof(buf), "PORT
%d,%d,%d,%d,%d,%d\r\n",
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=119
Status	New

The xmlNanoFTPList method calls the snprintf function, at line 1725 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1741	1741
Object	snprintf	snprintf

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1741.        snprintf(buf, sizeof(buf), "LIST -L\r\n");
```

Sizeof Pointer Argument

Query Path:

CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=535
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1640	1640
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1640.       buf[sizeof(buf) - 1] = 0;
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=536
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1752	1752
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.       buf[sizeof(buf) - 1] = 0;
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=537
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1752	1752
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.       buf[sizeof(buf) - 1] = 0;
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=538
Status	New

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	1752	1752
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.       buf[sizeof(buf) - 1] = 0;
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=539
Status	New

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1752	1752
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.       buf[sizeof(buf) - 1] = 0;
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=540
Status	New

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1752	1752
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.        buf[sizeof(buf) - 1] = 0;
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=541
Status	New

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	1752	1752
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.        buf[sizeof(buf) - 1] = 0;
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=542
Status	New

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	1752	1752

Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1752.       buf[sizeof(buf) - 1] = 0;
```

Sizeof Pointer Argument\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=543
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1629	1629
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1629.        snprintf(buf, sizeof(buf), "LIST -L\r\n");
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=544
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1638	1638
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1638.       snprintf(buf, sizeof(buf), "LIST -L %s\r\n", filename);
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=545
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1741	1741
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1741.       snprintf(buf, sizeof(buf), "LIST -L\r\n");
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=546
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1750	1750
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1750.       snprintf(buf, sizeof(buf), "LIST -L %s\r\n", filename);
```

Sizeof Pointer Argument\Path 13:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=547
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1741	1741
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1741.        snprintf(buf, sizeof(buf), "LIST -L\r\n");
```

Sizeof Pointer Argument\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=548
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1750	1750
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1750.        snprintf(buf, sizeof(buf), "LIST -L %s\r\n", filename);
```

Sizeof Pointer Argument\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=549
Status	New

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	1741	1741
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1741.        snprintf(buf, sizeof(buf), "LIST -L\r\n");
```

Sizeof Pointer Argument\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=550
Status New

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	1750	1750
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1750.        snprintf(buf, sizeof(buf), "LIST -L %s\r\n", filename);
```

Sizeof Pointer Argument\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=551
Status New

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1741	1741

Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1741.         snprintf(buf, sizeof(buf), "LIST -L\r\n");
```

Sizeof Pointer Argument\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=552
Status	New

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1750	1750
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1750.         snprintf(buf, sizeof(buf), "LIST -L %s\r\n", filename);
```

Sizeof Pointer Argument\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=553
Status	New

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1741	1741
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1741.        snprintf(buf, sizeof(buf), "LIST -L\r\n");
```

Sizeof Pointer Argument\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=554
Status	New

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1750	1750
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1750.        snprintf(buf, sizeof(buf), "LIST -L %s\r\n", filename);
```

Sizeof Pointer Argument\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=555
Status	New

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	1741	1741
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1741.        snprintf(buf, sizeof(buf), "LIST -L\r\n");
```

Sizeof Pointer Argument\Path 22:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=556
Status	New

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	1750	1750
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1750.        snprintf(buf, sizeof(buf), "LIST -L %s\r\n", filename);
```

Sizeof Pointer Argument\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=557
Status	New

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	1741	1741
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1741.        snprintf(buf, sizeof(buf), "LIST -L\r\n");
```

Sizeof Pointer Argument\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=558
Status	New

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	1750	1750
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1750.        snprintf(buf, sizeof(buf), "LIST -L %s\r\n", filename);
```

Sizeof Pointer Argument\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=559
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1681	1681
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1681.        if ((len = recv(ctxt->dataFd, &buf[indx], sizeof(buf) -
(indx + 1), 0)) < 0) {
```

Sizeof Pointer Argument\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=560
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1799	1799

Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1799.       if ((len = recv(ctxt->dataFd, &buf[indx], sizeof(buf) -
(indx + 1), 0)) < 0) {
```

Sizeof Pointer Argument\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=561
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1799	1799
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1799.       if ((len = recv(ctxt->dataFd, &buf[indx], sizeof(buf) -
(indx + 1), 0)) < 0) {
```

Sizeof Pointer Argument\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=562
Status	New

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	1799	1799
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c

Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1799.        if ((len = recv(ctxt->dataFd, &buf[indx], sizeof(buf) -
(indx + 1), 0)) < 0) {
```

Sizeof Pointer Argument\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=563
Status	New

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1799	1799
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1799.        if ((len = recv(ctxt->dataFd, &buf[indx], sizeof(buf) -
(indx + 1), 0)) < 0) {
```

Sizeof Pointer Argument\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=564
Status	New

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1799	1799
Object	buf	sizeof

Code Snippet

File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1799.        if ((len = recv(ctxt->dataFd, &buf[indx], sizeof(buf) -
(indx + 1), 0)) < 0) {
```

Sizeof Pointer Argument\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=565
Status	New

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	1799	1799
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1799.        if ((len = recv(ctxt->dataFd, &buf[indx], sizeof(buf) -
(indx + 1), 0)) < 0) {
```

Sizeof Pointer Argument\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=566
Status	New

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	1799	1799
Object	buf	sizeof

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1799.        if ((len = recv(ctxt->dataFd, &buf[indx], sizeof(buf) -
(indx + 1), 0)) < 0) {
```

TOCTOU

Query Path:

CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=919
Status	New

The main method in chromium@@chromium-120.0.6099.308-CVE-2021-3520-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	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1962	1962
Object	fopen	fopen

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
1962.        output = fopen("/tmp/tstdata", "w");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=920
Status	New

The main method in chromium@@chromium-86.0.4197.1-CVE-2021-3520-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	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	2095	2095
Object	fopen	fopen

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c

Method int main(int argc, char **argv) {

```
....
2095.       output = fopen("/tmp/tstdata", "w");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=921
Status	New

The main method in chromium@@chromium-86.0.4240.280-CVE-2021-3520-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	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	2095	2095
Object	fopen	fopen

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2095.       output = fopen("/tmp/tstdata", "w");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=922
Status	New

The main method in chromium@@chromium-88.0.4287.1-CVE-2021-3520-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	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	2095	2095
Object	fopen	fopen

Code Snippet

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2095.         output = fopen("/tmp/tstdata", "w");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=923
Status	New

The main method in chromium@@chromium-88.0.4324.218-CVE-2021-3520-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	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	2095	2095
Object	fopen	fopen

Code Snippet

File Name	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2095.         output = fopen("/tmp/tstdata", "w");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=924
Status	New

The main method in chromium@@chromium-89.0.4383.0-CVE-2021-3520-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	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	2095	2095
Object	fopen	fopen

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2095.       output = fopen("/tmp/tstdata", "w");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=925
Status	New

The main method in chromium@@chromium-94.0.4606.85-CVE-2021-3520-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	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	2095	2095
Object	fopen	fopen

Code Snippet
File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2095.       output = fopen("/tmp/tstdata", "w");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=926
Status	New

The main method in chromium@@chromium-97.0.4692.86-CVE-2021-3520-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	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	2095	2095
Object	fopen	fopen

Code Snippet	
File Name	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2095.       output = fopen("/tmp/tstdata", "w");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=927
Status	New

The ProcessProperties method in chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	172	172
Object	open	open

Code Snippet	
File Name	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method	int ProcessProperties(void) {

```
....
172.      s_tty_fd = open("/dev/tty", O_WRONLY);
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=928
Status	New

The ProcessProperties method in chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	212	212

Object	open	open

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method int ProcessProperties(void) {

```
....
212.     int fd0 = open(getenv("PS_STDIN"), O_RDONLY);
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=929
Status	New

The ProcessProperties method in chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	215	215
Object	open	open

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method int ProcessProperties(void) {

```
....
215.     int fd1 = open(getenv("PS_STDOUT"), O_WRONLY);
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=930
Status	New

The ProcessProperties method in chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c

Line	218	218
Object	open	open

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method int ProcessProperties(void) {

```
....
218.     int fd2 = open(getenv("PS_STDERR"), O_WRONLY);
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=931
Status	New

The MessageHandlerInput method in chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	280	280
Object	open	open

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method void MessageHandlerInput(struct PP_Var key,

```
....
280.     int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=932
Status	New

The ProcessProperties method in chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-	chromium@@chromium-122.0.6238.2-

	CVE-2021-44109-FP.c	CVE-2021-44109-FP.c
Line	172	172
Object	open	open

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method int ProcessProperties(void) {

```
....
172.        s_tty_fd = open("/dev/tty", O_WRONLY);
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=933
Status	New

The ProcessProperties method in chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	212	212
Object	open	open

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method int ProcessProperties(void) {

```
....
212.     int fd0 = open(getenv("PS_STDIN"), O_RDONLY);
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=934
Status	New

The ProcessProperties method in chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	215	215
Object	open	open

Code Snippet	
File Name	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method	int ProcessProperties(void) {

```
....
215.     int fd1 = open(getenv("PS_STDOUT"), O_WRONLY);
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=935
Status	New

The ProcessProperties method in chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	218	218
Object	open	open

Code Snippet	
File Name	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method	int ProcessProperties(void) {

```
....
218.     int fd2 = open(getenv("PS_STDERR"), O_WRONLY);
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=936
Status	New

The MessageHandlerInput method in chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	280	280
Object	open	open

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method void MessageHandlerInput(struct PP_Var key,

```
....
280.     int fd = open(filename, O_RDONLY);
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=937
Status	New

The ProcessProperties method in chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	172	172
Object	open	open

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method int ProcessProperties(void) {

```
....
172.       s_tty_fd = open("/dev/tty", O_WRONLY);
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=938
Status	New

The ProcessProperties method in chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	212	212
Object	open	open

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method int ProcessProperties(void) {

```
....
212.     int fd0 = open(getenv("PS_STDIN"), O_RDONLY);
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=939
Status	New

The ProcessProperties method in chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	215	215
Object	open	open

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method int ProcessProperties(void) {

```
....
215.     int fd1 = open(getenv("PS_STDOUT"), O_WRONLY);
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=940
Status	New

The ProcessProperties method in chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	218	218
Object	open	open

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method int ProcessProperties(void) {

```
....
218.     int fd2 = open(getenv("PS_STDERR"), O_WRONLY);
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=941
Status	New

The MessageHandlerInput method in chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	280	280
Object	open	open

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method void MessageHandlerInput(struct PP_Var key,

```
....
280.     int fd = open(filename, O_RDONLY);
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:
CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=898
Status	New

The system data read by xmlNanoFTPCloseConnection in the file chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c at line 1546 is potentially exposed by xmlNanoFTPCloseConnection found in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c at line 1546.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1564	1564
Object	perror	perror

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPCloseConnection(void *ctx) {

```
....
1564.       perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=899
Status	New

The system data read by xmlNanoFTPList in the file chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c at line 1725 is potentially exposed by xmlNanoFTPList found in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c at line 1725.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1779	1779
Object	perror	perror

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1779.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=900
Status	New

The system data read by xmlNanoFTPGet in the file chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c at line 1900 is potentially exposed by xmlNanoFTPGet found in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c at line 1900.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	1924	1924
Object	perror	perror

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGet(void *ctx, ftpDataCallback callback, void *userData,

```
....
1924.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=901
Status	New

The system data read by xmlNanoFTPCloseConnection in the file chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c at line 1546 is potentially exposed by xmlNanoFTPCloseConnection found in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c at line 1546.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1564	1564
Object	perror	perror

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPCloseConnection(void *ctx) {

```
....
1564.       perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=902
Status	New

The system data read by xmlNanoFTPList in the file chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c at line 1725 is potentially exposed by xmlNanoFTPList found in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c at line 1725.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1779	1779
Object	perror	perror

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1779.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=903
Status	New

The system data read by xmlNanoFTPGet in the file chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c at line 1900 is potentially exposed by xmlNanoFTPGet found in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c at line 1900.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	1924	1924
Object	perror	perror

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPGet(void *ctx, ftpDataCallback callback, void *userData,

```
....
1924.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=904
Status	New

The system data read by xmlNanoFTPCloseConnection in the file chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c at line 1546 is potentially exposed by xmlNanoFTPCloseConnection found in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c at line 1546.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	1564	1564
Object	perror	perror

Code Snippet

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPCloseConnection(void *ctx) {

```
....
1564.       perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=905
Status	New

The system data read by xmlNanoFTPList in the file chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c at line 1725 is potentially exposed by xmlNanoFTPList found in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c at line 1725.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	1779	1779
Object	perror	perror

Code Snippet

File Name	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1779.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=906
Status	New

The system data read by xmlNanoFTPGet in the file chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c at line 1900 is potentially exposed by xmlNanoFTPGet found in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c at line 1900.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	1924	1924
Object	perror	perror

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPGet(void *ctx, ftpDataCallback callback, void *userData,

```
....
1924.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=907
Status	New

The system data read by xmlNanoFTPCloseConnection in the file chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c at line 1546 is potentially exposed by xmlNanoFTPCloseConnection found in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c at line 1546.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1564	1564
Object	perror	perror

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c

Method	xmlNanoFTPCloseConnection(void *ctx) {

```
....
1564.          perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=908
Status	New

The system data read by xmlNanoFTPList in the file chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c at line 1725 is potentially exposed by xmlNanoFTPList found in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c at line 1725.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1779	1779
Object	perror	perror

Code Snippet	
File Name	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1779.            perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=909
Status	New

The system data read by xmlNanoFTPGet in the file chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c at line 1900 is potentially exposed by xmlNanoFTPGet found in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c at line 1900.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	1924	1924
Object	perror	perror

Code Snippet

File Name	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method	xmlNanoFTPGet(void *ctx, ftpDataCallback callback, void *userData,

```
....
1924.            perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=910
Status	New

The system data read by xmlNanoFTPCloseConnection in the file chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c at line 1546 is potentially exposed by xmlNanoFTPCloseConnection found in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c at line 1546.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1564	1564
Object	perror	perror

Code Snippet

File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	xmlNanoFTPCloseConnection(void *ctx) {

```
....
1564.        perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=911
Status	New

The system data read by xmlNanoFTPList in the file chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c at line 1725 is potentially exposed by xmlNanoFTPList found in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c at line 1725.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1779	1779
Object	perror	perror

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1779.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=912
Status	New

The system data read by xmlNanoFTPGet in the file chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c at line 1900 is potentially exposed by xmlNanoFTPGet found in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c at line 1900.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	1924	1924
Object	perror	perror

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPGet(void *ctx, ftpDataCallback callback, void *userData,

```
....
1924.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=913
Status	New

The system data read by xmlNanoFTPCloseConnection in the file chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c at line 1546 is potentially exposed by xmlNanoFTPCloseConnection found in chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c at line 1546.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	1564	1564
Object	perror	perror

Code Snippet

File Name	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method	xmlNanoFTPCloseConnection(void *ctx) {

```
....
1564.       perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=914
Status	New

The system data read by xmlNanoFTPList in the file chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c at line 1725 is potentially exposed by xmlNanoFTPList found in chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c at line 1725.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	1779	1779
Object	perror	perror

Code Snippet

File Name	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method	xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1779.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=915
Status	New

The system data read by xmlNanoFTPGet in the file chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c at line 1900 is potentially exposed by xmlNanoFTPGet found in chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c at line 1900.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	1924	1924

Object	perror	perror

Code Snippet
File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method xmlNanoFTPGet(void *ctx, ftpDataCallback callback, void *userData,

```
....
1924.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=916
Status	New

The system data read by xmlNanoFTPCloseConnection in the file chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c at line 1546 is potentially exposed by xmlNanoFTPCloseConnection found in chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c at line 1546.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	1564	1564
Object	perror	perror

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method xmlNanoFTPCloseConnection(void *ctx) {

```
....
1564.       perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=917
Status	New

The system data read by xmlNanoFTPList in the file chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c at line 1725 is potentially exposed by xmlNanoFTPList found in chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c at line 1725.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c

Line	1779	1779
Object	perror	perror

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method xmlNanoFTPList(void *ctx, ftpListCallback callback, void *userData,

```
....
1779.           perror("select");
```

Exposure of System Data to Unauthorized Control Sphere\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=918
Status	New

The system data read by xmlNanoFTPGet in the file chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c at line 1900 is potentially exposed by xmlNanoFTPGet found in chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c at line 1900.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	1924	1924
Object	perror	perror

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method xmlNanoFTPGet(void *ctx, ftpDataCallback callback, void *userData,

```
....
1924.           perror("select");
```

Incorrect Permission Assignment For Critical Resources

Query Path:
CPP\Cx\CPP Low Visibility\Incorrect Permission Assignment For Critical Resources Version:1

Categories

FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Incorrect Permission Assignment For Critical Resources\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&

	pathid=879
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1962	1962
Object	output	output

Code Snippet

File Name	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
1962.       output = fopen("/tmp/tstdata", "w");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=880
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	2095	2095
Object	output	output

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2095.       output = fopen("/tmp/tstdata", "w");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=881
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c

Line	2095	2095
Object	output	output

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2095.       output = fopen("/tmp/tstdata", "w");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=882
Status	New

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	2095	2095
Object	output	output

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method int main(int argc, char **argv) {

```
....
2095.       output = fopen("/tmp/tstdata", "w");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=883
Status	New

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	2095	2095
Object	output	output

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c

Method	int main(int argc, char **argv) {

```
....
2095.        output = fopen("/tmp/tstdata", "w");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=884
Status	New

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	2095	2095
Object	output	output

Code Snippet	
File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2095.        output = fopen("/tmp/tstdata", "w");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=885
Status	New

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	2095	2095
Object	output	output

Code Snippet	
File Name	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2095.        output = fopen("/tmp/tstdata", "w");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=886
Status	New

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	2095	2095
Object	output	output

Code Snippet

File Name	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method	int main(int argc, char **argv) {

```
....
2095.       output = fopen("/tmp/tstdata", "w");
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=887
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Line	763	763
Object	mkdir	mkdir

Code Snippet

File Name	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20032-TP.c
Method	int cli_scanhfsplus(cli_ctx *ctx)

```
....
763.       if (mkdir(targetdir, 0700)) {
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=888
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c
Line	162	162
Object	mkdir	mkdir

Code Snippet

File Name Cisco-Talos@@clamav-clamav-0.102.3-CVE-2023-20052-TP.c

Method int cli_scandmg(cli_ctx *ctx)

```
....
162.        if (mkdir(dirname, 0700)) {
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=889
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c
Line	1484	1484
Object	mkdir	mkdir

Code Snippet

File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20032-TP.c

Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1484.        if (mkdir(targetdir, 0700)) {
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=890
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Line	162	162

Object	mkdir	mkdir

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
162.        if (mkdir(dirname, 0700)) {
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=891
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c
Line	1484	1484
Object	mkdir	mkdir

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20032-TP.c
Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1484.        if (mkdir(targetdir, 0700)) {
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=892
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c
Line	162	162
Object	mkdir	mkdir

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.1-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
162.        if (mkdir(dirname, 0700)) {
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=893
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c
Line	1484	1484
Object	mkdir	mkdir

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20032-TP.c
Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1484.        if (mkdir(targetdir, 0700)) {
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=894
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c
Line	162	162
Object	mkdir	mkdir

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.3-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
162.        if (mkdir(dirname, 0700)) {
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=895
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c
Line	1484	1484
Object	mkdir	mkdir

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20032-TP.c
Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1484.       if (mkdir(targetdir, 0700)) {
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=896
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c	Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c
Line	162	162
Object	mkdir	mkdir

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.4-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
162.        if (mkdir(dirname, 0700)) {
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=897
Status	New

	Source	Destination
File	Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c	Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c
Line	1484	1484
Object	mkdir	mkdir

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20032-TP.c
Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1484.       if (mkdir(targetdir, 0700)) {
```

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	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=519
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c line 771, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	805	805
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
805.            if (getaddrinfo (proxy, NULL, &hints, &result) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=520
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 771 of chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c line 771, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	811	811
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
811.            if (getaddrinfo (ctxt->hostname, NULL, &hints, &result)
!= 0) {
```

Reliance on DNS Lookups in a Decision\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=521
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	883	883
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
883.            if (getaddrinfo (proxy, NULL, &hints, &result) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=522
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	889	889
Object	getaddrinfo	!=

Code Snippet

File Name	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method	xmlNanoFTPConnect(void *ctx) {

```
....
889.            if (getaddrinfo (ctxt->hostname, NULL, &hints, &result)
!= 0) {
```

Reliance on DNS Lookups in a Decision\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=523
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	883	883
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
883.            if (getaddrinfo (proxy, NULL, &hints, &result) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=524
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	889	889
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
889.            if (getaddrinfo (ctxt->hostname, NULL, &hints, &result)
!= 0) {
```

Reliance on DNS Lookups in a Decision\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=525
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-	chromium@@chromium-88.0.4287.1-

	CVE-2021-3520-FP.c	CVE-2021-3520-FP.c
Line	883	883
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
883.            if (getaddrinfo (proxy, NULL, &hints, &result) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=526
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	889	889
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
889.            if (getaddrinfo (ctxt->hostname, NULL, &hints, &result)
!= 0) {
```

Reliance on DNS Lookups in a Decision\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=527
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	883	883
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
883.            if (getaddrinfo (proxy, NULL, &hints, &result) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=528
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	889	889
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
889.            if (getaddrinfo (ctxt->hostname, NULL, &hints, &result)
!= 0) {
```

Reliance on DNS Lookups in a Decision\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=529
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	883	883
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
883.            if (getaddrinfo (proxy, NULL, &hints, &result) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=530
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	889	889
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
889.            if (getaddrinfo (ctxt->hostname, NULL, &hints, &result)
!= 0) {
```

Reliance on DNS Lookups in a Decision\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=531
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	883	883
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
883.            if (getaddrinfo (proxy, NULL, &hints, &result) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=532
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	889	889
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
889.            if (getaddrinfo (ctxt->hostname, NULL, &hints, &result)
!= 0) {
```

Reliance on DNS Lookups in a Decision\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=533
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	883	883
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
883.            if (getaddrinfo (proxy, NULL, &hints, &result) != 0) {
```

Reliance on DNS Lookups in a Decision\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=534
Status	New

The xmlNanoFTPConnect method performs a reverse DNS lookup with getaddrinfo, at line 849 of chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c. The application then makes a security decision, !=, in chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c line 849, even though this hostname is not reliable and can be easily spoofed.

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	889	889
Object	getaddrinfo	!=

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method xmlNanoFTPConnect(void *ctx) {

```
....
889.             if (getaddrinfo (ctxt->hostname, NULL, &hints, &result)
!= 0) {
```

Improper Resource Access Authorization

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=868
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	428	428
Object	fprintf	fprintf

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method static void VALog(enum PSVerbosity verbosity, const char* fmt, va_list args) {

```
....
428.      fprintf(stderr, "ps: ");
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=869
Status	New

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	428	428
Object	fprintf	fprintf

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method static void VALog(enum PSVerbosity verbosity, const char* fmt, va_list args) {

```
....
428.       fprintf(stderr, "ps: ");
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=870
Status	New

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	428	428
Object	fprintf	fprintf

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method static void VALog(enum PSVerbosity verbosity, const char* fmt, va_list args) {

```
....
428.       fprintf(stderr, "ps: ");
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=871
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Line	1936	1936
Object	fwrite	fwrite

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-3520-FP.c
Method void ftpData(void *userData, const char *data, int len) {

```
....
1936.       fwrite(data, len, 1, (FILE*)userData);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=872
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Line	2069	2069
Object	fwrite	fwrite

Code Snippet
File Name chromium@@chromium-86.0.4197.1-CVE-2021-3520-FP.c
Method void ftpData(void *userData, const char *data, int len) {

```
....
2069.       fwrite(data, len, 1, (FILE*)userData);
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=873
Status	New

	Source	Destination
File	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c	chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Line	2069	2069
Object	fwrite	fwrite

Code Snippet
File Name chromium@@chromium-86.0.4240.280-CVE-2021-3520-FP.c
Method void ftpData(void *userData, const char *data, int len) {

```
....
2069.       fwrite(data, len, 1, (FILE*)userData);
```

Improper Resource Access Authorization\Path 7:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=874
Status	New

	Source	Destination
File	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Line	2069	2069
Object	fwrite	fwrite

Code Snippet
File Name chromium@@chromium-88.0.4287.1-CVE-2021-3520-FP.c
Method void ftpData(void *userData, const char *data, int len) {

```
....
2069.       fwrite(data, len, 1, (FILE*)userData);
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=875
Status	New

	Source	Destination
File	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c	chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Line	2069	2069
Object	fwrite	fwrite

Code Snippet
File Name chromium@@chromium-88.0.4324.218-CVE-2021-3520-FP.c
Method void ftpData(void *userData, const char *data, int len) {

```
....
2069.       fwrite(data, len, 1, (FILE*)userData);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=876
Status	New

	Source	Destination
File	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Line	2069	2069
Object	fwrite	fwrite

Code Snippet

File Name	chromium@@chromium-89.0.4383.0-CVE-2021-3520-FP.c
Method	void ftpData(void *userData, const char *data, int len) {

```
....
2069.       fwrite(data, len, 1, (FILE*)userData);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=877
Status	New

	Source	Destination
File	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Line	2069	2069
Object	fwrite	fwrite

Code Snippet

File Name	chromium@@chromium-94.0.4606.85-CVE-2021-3520-FP.c
Method	void ftpData(void *userData, const char *data, int len) {

```
....
2069.       fwrite(data, len, 1, (FILE*)userData);
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=878
Status	New

	Source	Destination
File	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c	chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Line	2069	2069

Object	fwrite	fwrite

Code Snippet
File Name chromium@@chromium-97.0.4692.86-CVE-2021-3520-FP.c
Method void ftpData(void *userData, const char *data, int len) {

```
....
2069.       fwrite(data, len, 1, (FILE*)userData);
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=277
Status	New

	Source	Destination
File	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c	chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Line	101	101
Object	sizeof	sizeof

Code Snippet
File Name chromium@@chromium-120.0.6099.308-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
101.    si->argv_ = calloc(argc + 1, sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=278
Status	New

	Source	Destination
File	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c	chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Line	101	101
Object	sizeof	sizeof

Code Snippet
File Name chromium@@chromium-122.0.6238.2-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
101.    si->argv_ = calloc(argc + 1, sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000010&projectid=6&pathid=279
Status	New

	Source	Destination
File	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c	chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Line	101	101
Object	sizeof	sizeof

Code Snippet
File Name chromium@@chromium-127.0.6533.45-CVE-2021-44109-FP.c
Method static PP_Bool Instance_DidCreate(PP_Instance instance,

```
....
101.    si->argv_ = calloc(argc + 1, sizeof(char*));
```

Buffer Overflow Indexes

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Buffer Overflow boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```cpp
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

Validating Destination Buffer Length

```cpp
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
      int i;
      i = 1;
      return &i;
}

void func2()
```

```
{
        int j;
        j = 5;
}

//..
        int * i = func1();
        printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
        func2();
        printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

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;
}
```

Improper Sanitization of Special Elements used in a Command ('Command Injection')

Weakness ID: 77 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not sanitize or incorrectly sanitizes special elements that could modify the intended command when it is sent to a downstream component.

Extended Description

Command injection vulnerabilities typically occur when:

1. Data enters the application from an untrusted source.

2. The data is part of a string that is executed as a command by the application.

3. By executing the command, the application gives an attacker a privilege or capability that the attacker would not otherwise have.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Access Control	Command injection allows for the execution of arbitrary commands and code by the attacker.
Integrity	If a malicious user injects a character (such as a semi-colon) that delimits the end of one command and the beginning of another, it may be possible to then insert an entirely new and unrelated command that was not intended to be executed.

Likelihood of Exploit

Very High

Demonstrative Examples

Example 1

The following simple program accepts a filename as a command line argument and displays the contents of the file back to the user. The program is installed setuid root because it is intended for use as a learning tool to allow system administrators in-training to inspect privileged system files without giving them the ability to modify them or damage the system.

Example Language: **C**

```
int main(char* argc, char** argv) {
char cmd[CMD_MAX] = "/usr/bin/cat ";
strcat(cmd, argv[1]);
system(cmd);
}
```

Because the program runs with root privileges, the call to system() also executes with root privileges. If a user specifies a standard filename, the call works as expected. However, if an attacker passes a string of the form ";rm -rf /", then the call to system() fails to execute cat due to a lack of arguments and then plows on to recursively delete the contents of the root partition.

Example 2

The following code is from an administrative web application designed to allow users to kick off a backup of an Oracle database using a batch-file wrapper around the rman utility and then run a cleanup.bat script to delete some temporary files. The script rmanDB.bat accepts a single command line parameter, which specifies what type of backup to perform. Because access to the database is restricted, the application runs the backup as a privileged user.

(Bad Code)

Example Language: **Java**

```
...
String btype = request.getParameter("backuptype");
String cmd = new String("cmd.exe /K \"
c:\\util\\rmanDB.bat "
+btype+
"&&c:\\utl\\cleanup.bat\"")
System.Runtime.getRuntime().exec(cmd);
...
```

The problem here is that the program does not do any validation on the backuptype parameter read from the user. Typically the Runtime.exec() function will not execute multiple commands, but in this case the program first runs the cmd.exe shell in order to run multiple commands with a single call to Runtime.exec(). Once the shell is invoked, it will happily execute multiple commands separated by two ampersands. If an attacker passes a string of the form "& del c:\\dbms\\*.*", then the application will execute this command along with the others specified by the program. Because of the nature of the application, it runs with the privileges necessary to interact with the database, which means whatever command the attacker injects will run with those privileges as well.

Example 3

The following code from a system utility uses the system property APPHOME to determine the directory in which it is installed and then executes an initialization script based on a relative path from the specified directory.

(Bad Code)

Example Language: **Java**

```
...
String home = System.getProperty("APPHOME");
String cmd = home + INITCMD;
java.lang.Runtime.getRuntime().exec(cmd);
...
```

The code above allows an attacker to execute arbitrary commands with the elevated privilege of the application by modifying the system property APPHOME to point to a different path containing a malicious version of INITCMD. Because the program does not validate the value read from the environment, if an attacker can control the value of the system property APPHOME, then they can fool the application into running malicious code and take control of the system.

Example 4

The following code is from a web application that allows users access to an interface through which they can update their password on the system. Part of the process for updating passwords in certain network environments is to run a make command in the /var/yp directory, the code for which is shown below.

(Bad Code)

Example Language: **Java**

```
...
System.Runtime.getRuntime().exec("make");
...
```

The problem here is that the program does not specify an absolute path for make and fails to clean its environment prior to executing the call to Runtime.exec(). If an attacker can modify the $PATH variable to point to a malicious binary called make and cause the program to be executed in their environment, then the malicious binary will be loaded instead of the one intended. Because of the nature of the application, it runs with the privileges necessary to perform system operations, which means the attacker's make will now be run with these privileges, possibly giving the attacker complete control of the system.

Example 5

The following code is a wrapper around the UNIX command cat which prints the contents of a file to standard out. It is also injectable:

(Bad Code)

Example Language: ***C***

```c
#include <stdio.h>
#include <unistd.h>

int main(int argc, char **argv) {

char cat[] = "cat ";
char *command;
size_t commandLength;

commandLength = strlen(cat) + strlen(argv[1]) + 1;
command = (char *) malloc(commandLength);
strncpy(command, cat, commandLength);
strncat(command, argv[1], (commandLength - strlen(cat)) );

system(command);
return (0);
}
```

Used normally, the output is simply the contents of the file requested:

```
$ ./catWrapper Story.txt
When last we left our heroes...
```

However, if we add a semicolon and another command to the end of this line, the command is executed by catWrapper with no complaint:

(Attack)

```
$ ./catWrapper Story.txt; ls
When last we left our heroes...
Story.txt
SensitiveFile.txt
PrivateData.db
a.out*
```

If catWrapper had been set to have a higher privilege level than the standard user, arbitrary commands could be executed with that higher privilege.

Potential Mitigations

Phase: Architecture and Design

If at all possible, use library calls rather than external processes to recreate the desired functionality

Phase: Implementation

If possible, ensure that all external commands called from the program are statically created.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

Run time: Run time policy enforcement may be used in a white-list fashion to prevent use of any non-sanctioned commands.

Assign permissions to the software system that prevents the user from accessing/opening privileged files.

Other Notes

Command injection is a common problem with wrapper programs.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	74	Failure to Sanitize Data into a Different Plane ('Injection')	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	713	OWASP Top Ten 2007 Category A2 - Injection Flaws	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	Weaknesses in OWASP Top Ten (2004)711
ChildOf	Category	727	OWASP Top Ten 2004 Category A6 - Injection Flaws	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ParentOf	Weakness Base	78	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	88	Argument Injection or Modification	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	89	Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	90	Failure to Sanitize Data into LDAP Queries ('LDAP Injection')	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ParentOf	Weakness Base	624	Executable Regular Expression Error	**Development Concepts (primary)699** **Research Concepts (primary)1000**

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Command Injection
CLASP			Command injection

OWASP Top Ten 2007	A2	CWE More Specific	Injection Flaws
OWASP Top Ten 2004	A1	CWE More Specific	Unvalidated Input
OWASP Top Ten 2004	A6	CWE More Specific	Injection Flaws

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
15	Command Delimiters	
23	File System Function Injection, Content Based	
43	Exploiting Multiple Input Interpretation Layers	
75	Manipulating Writeable Configuration Files	
6	Argument Injection	
11	Cause Web Server Misclassification	
76	Manipulating Input to File System Calls	

References

G. Hoglund and G. McGraw. "Exploiting Software: How to Break Code". Addison-Wesley. February 2004.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Name		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Name		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Other Notes, Potential Mitigations		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Command Injection
2009-05-27	Failure to Sanitize Data into a Control Plane (aka 'Command Injection')
2009-07-27	Failure to Sanitize Data into a Control Plane ('Command Injection')

BACK TO TOP

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```

/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

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(ServletRequest req) {
      boolean isCompany = false;

      Principal user = req.getUserPrincipal();
      if (user != null) {
      if (user.getName().startsWith(COMPANYDOMAIN + "\\")) {
             isCompany = true;
         }
     }
      return isCompany;
}
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```

/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699** **Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Missing or Inconsistent Access Control

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions

Submission Date	Submitter	Organization	Source
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		

Modifications

Modification Date	Modifier	Organization	Source
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Insecure Permission Assignment for Resource
2009-05-27	Insecure Permission Assignment for Critical Resource

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
        public static int counter = 0;
        public static void start() throws InterruptedException {
               incrementCounter ic;
               decrementCounter dc;
               while(counter == 0) {
                      counter = 0;
                      ic = new incrementCounter();
                      dc = new decrementCounter();
                      ic.start();
                      dc.start();
                      ic.join();
                      dc.join();
               }
               System.out.println(counter); //Will stop and return either -1 or 1 due to race
  condition over counter
        }

        public static class incrementCounter extends Thread {
            public void run() {
               counter++;
            }
        }

        public static class decrementCounter extends Thread {
            public void run() {
               counter--;
            }
        }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
        public static int counter = 0;
        public static Object lock = new Object();

        public static void start() throws InterruptedException {
               incrementCounter ic;
               decrementCounter dc;
               while(counter == 0) { // because of proper locking, this condition is never false
                      counter = 0;
                      ic = new incrementCounter();
                      dc = new decrementCounter();
                      ic.start();
                      dc.start();
                      ic.join();
                      dc.join();
               }
               System.out.println(counter); // Never reached
        }

        public static class incrementCounter extends Thread {
            public void run() {
               synchronized (lock) {
                      counter++;
               }
            }
        }

        public static class decrementCounter extends Thread {
            public void run() {
               synchronized (lock) {
                      counter--;
               }
            }
        }
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025