vul_files_26 Scan Report

Project Name	vul_files_26
Scan Start	Tuesday, January 7, 2025 2:31:31 PM
Preset	Checkmarx Default
Scan Time	01h:30m:37s
Lines Of Code Scanned	296821
Files Scanned	86
Report Creation Time	Tuesday, January 7, 2025 3:09:27 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	1/1000 (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

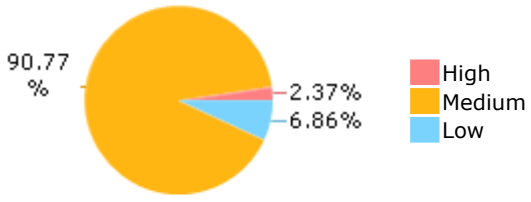
Results Limit

Results limit per query was set to 50

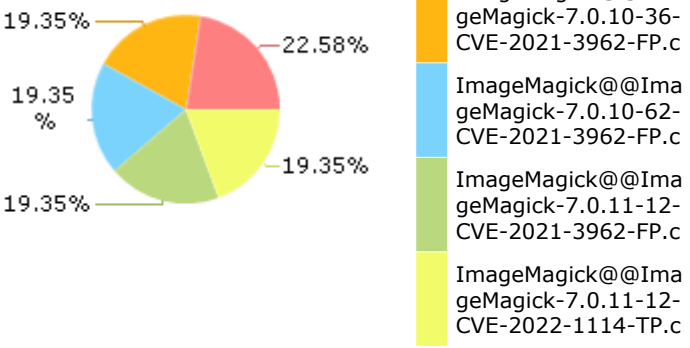
Selected Queries

Selected queries are listed in Result Summary

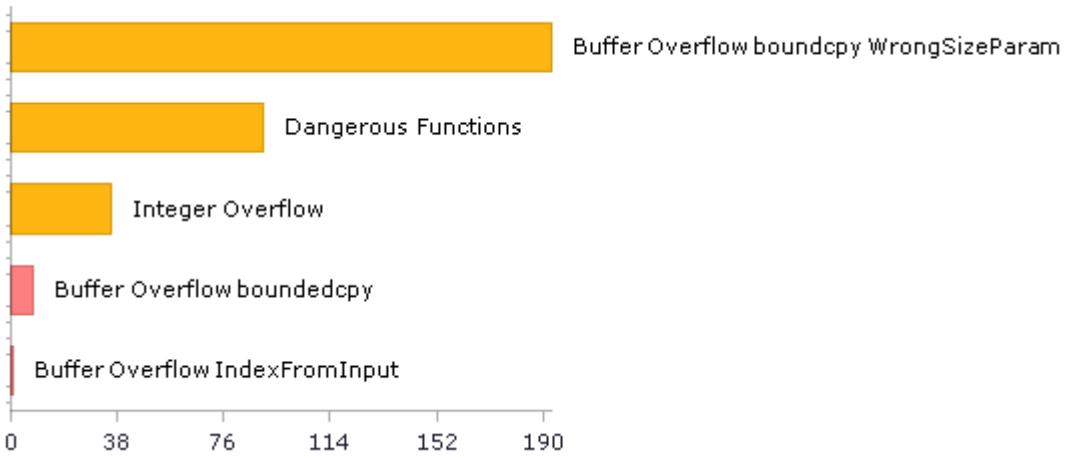
Result Summary



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	216	215
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	10	10
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	90	90
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	90	90
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	10	10
PCI DSS (3.2) - 6.5.2 - Buffer overflows	237	237
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.	1	1
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	9	9
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.	36	36

***** 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)	10	10
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	17	16
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	45	45
SI-11 Error Handling (P2)*	2	2
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	10	10

***** 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

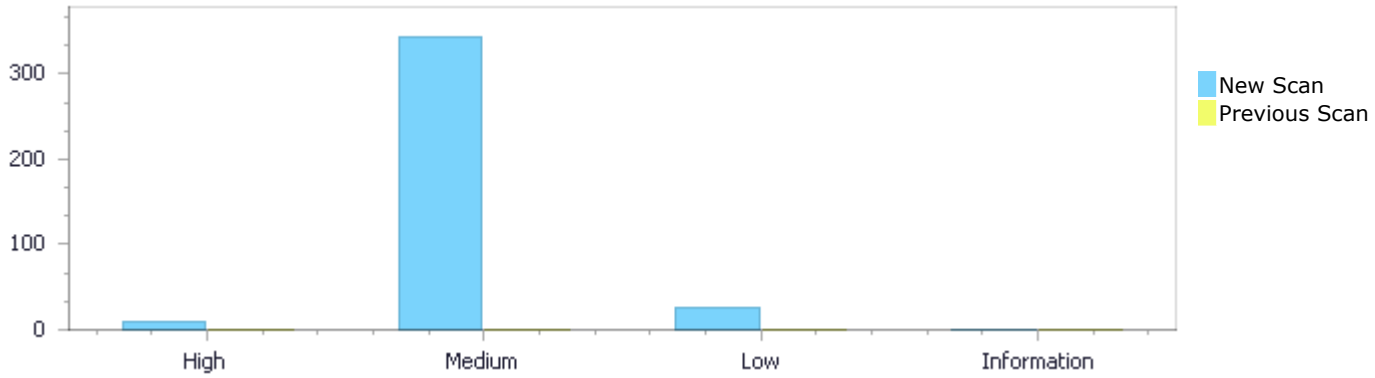
Scan Summary - Custom

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	9	344	26	0	379
Recurrent Issues	0	0	0	0	0
Total	9	344	26	0	379
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	9	344	26	0	379
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	9	344	26	0	379

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow boundedcpy	8	High
Buffer Overflow IndexFromInput	1	High
Buffer Overflow boundcpy WrongSizeParam	193	Medium
Dangerous Functions	90	Medium
Integer Overflow	36	Medium

Memory Leak	12	Medium
MemoryFree on StackVariable	7	Medium
Use After Free	3	Medium
Wrong Size t Allocation	2	Medium
Use of Zero Initialized Pointer	1	Medium
Potential Off by One Error in Loops	10	Low
Improper Resource Access Authorization	9	Low
TOCTOU	2	Low
Unchecked Return Value	2	Low
Incorrect Permission Assignment For Critical Resources	1	Low
NULL Pointer Dereference	1	Low
Unchecked Array Index	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	22
ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	22
ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	22
ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	22
heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	19
ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c	19
ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c	19
ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c	18
ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c	18
ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c	18

Scan Results Details

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=1010039&projectid=10028&pathid=1
Status	New

The size parameter sizeof in line 897 in file ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c is influenced by the user input cin in line 897 in file ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Line	965	965
Object	cin	sizeof

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
965.     (void) memset(&cin,0,sizeof(cin));
```

Buffer Overflow boundedcpy\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=2
Status	New

The size parameter sizeof in line 380 in file ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c is influenced by the user input cin in line 380 in file ImageMagick@@ImageMagick-7.0.10-25-CVE-

2022-28463-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Line	450	450
Object	cin	sizeof

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Method static Image *ReadCINImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
450.     memset(&cin,0,sizeof(cin));
```

Buffer Overflow boundedcpy\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=3
Status New

The size parameter sizeof in line 897 in file ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c is influenced by the user input cin in line 897 in file ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Line	965	965
Object	cin	sizeof

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
965.     (void) memset(&cin,0,sizeof(cin));
```

Buffer Overflow boundedcpy\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10

	028&pathid=4
Status	New

The size parameter sizeof in line 380 in file ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c is influenced by the user input cin in line 380 in file ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Line	450	450
Object	cin	sizeof

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Method static Image *ReadCINImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
450.    memset(&cin,0,sizeof(cin));
```

Buffer Overflow boundedcpy\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=5
Status	New

The size parameter sizeof in line 897 in file ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c is influenced by the user input cin in line 897 in file ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Line	965	965
Object	cin	sizeof

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
965.    (void) memset(&cin,0,sizeof(cin));
```

Buffer Overflow boundedcpy\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=6
Status	New

The size parameter sizeof in line 380 in file ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c is influenced by the user input cin in line 380 in file ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Line	450	450
Object	cin	sizeof

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c

Method static Image *ReadCINImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
450.    memset(&cin,0,sizeof(cin));
```

Buffer Overflow boundedcpy\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=7
Status	New

The size parameter sizeof in line 897 in file ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c is influenced by the user input cin in line 897 in file ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Line	965	965
Object	cin	sizeof

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c

Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
965.     (void) memset(&cin,0,sizeof(cin));
```

Buffer Overflow boundedcpy\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=8
Status	New

The size parameter sizeof in line 380 in file ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c is influenced by the user input cin in line 380 in file ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Line	450	450
Object	cin	sizeof

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c

Method static Image *ReadCINImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
450.     memset(&cin,0,sizeof(cin));
```

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=1010039&projectid=10028&pathid=9
Status	New

The size of the buffer used by load_mappings in strcspn, at line 1865 of heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that load_mappings passes to buf, at line 1865 of heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c, to overwrite the target buffer.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1876	1879
Object	buf	strcspn

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1876.       while (fgets(buf, sizeof(buf), f) != NULL) {
....
1879.        buf[strcspn(buf, "\n")] = '\0';
```

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=1010039&projectid=10028&pathid=20
Status	New

The size of the buffer used by *ReadDCMImage in info, at line 3003 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadDCMImage passes to info, at line 3003 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Line	3249	3249
Object	info	info

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3249.             memcpy(info_copy,&info,sizeof(info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=21
Status	New

The size of the buffer used by *ReadDCMImage in info, at line 3003 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadDCMImage passes to info, at line 3003 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	3249	3249
Object	info	info

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3249.            memcpy(info_copy,&info,sizeof(info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=22
Status	New

The size of the buffer used by *ReadDCMImage in info, at line 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadDCMImage passes to info, at line 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	3251	3251
Object	info	info

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3251.           memcpy(info_copy,&info,sizeof(info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=23
Status	New

The size of the buffer used by *ReadDCMImage in info, at line 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadDCMImage passes to info, at line 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	3251	3251
Object	info	info

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c

Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3251.           memcpy(info_copy,&info,sizeof(info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=24
Status	New

The size of the buffer used by gif_create in gif_animation, at line 920 of hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gif_create passes to gif_animation, at line 920 of hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c, to overwrite the target buffer.

	Source	Destination
File	hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c	hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c
Line	922	922
Object	gif_animation	gif_animation

Code Snippet

File Name	hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c
Method	void gif_create(gif_animation *gif, gif_bitmap_callback_vt *bitmap_callbacks)

```
....
922.          memset(gif, 0, sizeof(gif_animation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=25
Status	New

The size of the buffer used by gif_create in gif_animation, at line 921 of hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gif_create passes to gif_animation, at line 921 of hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c, to overwrite the target buffer.

	Source	Destination
File	hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c	hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c
Line	923	923
Object	gif_animation	gif_animation

Code Snippet

File Name	hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c
Method	void gif_create(gif_animation *gif, gif_bitmap_callback_vt *bitmap_callbacks)

```
....
923.          memset(gif, 0, sizeof(gif_animation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=26
Status	New

The size of the buffer used by gif_create in gif_animation, at line 921 of hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gif_create passes to gif_animation, at line 921 of hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c, to overwrite the target buffer.

	Source	Destination
File	hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c	hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c
Line	923	923
Object	gif_animation	gif_animation

Code Snippet	
File Name	hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c
Method	void gif_create(gif_animation *gif, gif_bitmap_callback_vt *bitmap_callbacks)

```
....
923.          memset(gif, 0, sizeof(gif_animation));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=27
Status	New

The size of the buffer used by WriteCINImage in Namespace1285313767, at line 897 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1285313767, at line 897 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Line	1000	1000
Object	Namespace1285313767	Namespace1285313767

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Method	static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1000.     (void)
memset(cin.file.create_date,0,sizeof(cin.file.create_date));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=28
Status	New

The size of the buffer used by WriteCINImage in Namespace1285313767, at line 897 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1285313767, at line 897 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-	ImageMagick@@ImageMagick-7.0.10-

	25-CVE-2022-28463-FP.c	25-CVE-2022-28463-FP.c
Line	1004	1004
Object	Namespace1285313767	Namespace1285313767

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1004.     (void)
memset(cin.file.create_time,0,sizeof(cin.file.create_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=29
Status	New

The size of the buffer used by WriteCINImage in Namespace1285313767, at line 897 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1285313767, at line 897 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Line	1098	1098
Object	Namespace1285313767	Namespace1285313767

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1098.       sizeof(cin.origination.create_date));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=30
Status	New

The size of the buffer used by WriteCINImage in Namespace1285313767, at line 897 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1285313767, at line 897 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Line	1103	1103
Object	Namespace1285313767	Namespace1285313767

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1103.       sizeof(cin.origination.create_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=31
Status New

The size of the buffer used by *ReadCINImage in Namespace1285313767, at line 380 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadCINImage passes to Namespace1285313767, at line 380 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Line	626	626
Object	Namespace1285313767	Namespace1285313767

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-28463-FP.c
Method static Image *ReadCINImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
626.      sizeof(cin.origination.serial));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=32
Status	New

The size of the buffer used by WriteCINImage in Namespace995946675, at line 897 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace995946675, at line 897 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Line	1000	1000
Object	Namespace995946675	Namespace995946675

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1000.     (void)
memset(cin.file.create_date,0,sizeof(cin.file.create_date));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=33
Status	New

The size of the buffer used by WriteCINImage in Namespace995946675, at line 897 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace995946675, at line 897 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Line	1004	1004
Object	Namespace995946675	Namespace995946675

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1004.    (void)
memset(cin.file.create_time,0,sizeof(cin.file.create_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=34
Status	New

The size of the buffer used by WriteCINImage in Namespace995946675, at line 897 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace995946675, at line 897 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Line	1098	1098
Object	Namespace995946675	Namespace995946675

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c

Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1098.      sizeof(cin.origination.create_date));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=35
Status	New

The size of the buffer used by WriteCINImage in Namespace995946675, at line 897 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace995946675, at line 897 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Line	1103	1103

Object	Namespace995946675	Namespace995946675

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1103.       sizeof(cin.origination.create_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=36
Status	New

The size of the buffer used by *ReadCINImage in Namespace995946675, at line 380 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadCINImage passes to Namespace995946675, at line 380 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Line	626	626
Object	Namespace995946675	Namespace995946675

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-28463-FP.c
Method static Image *ReadCINImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
626.      sizeof(cin.origination.serial));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=37
Status	New

The size of the buffer used by WriteCINImage in Namespace1656850520, at line 897 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1656850520, at line 897 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Line	1000	1000
Object	Namespace1656850520	Namespace1656850520

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1000.     (void)
memset(cin.file.create_date,0,sizeof(cin.file.create_date));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=38
Status New

The size of the buffer used by WriteCINImage in Namespace1656850520, at line 897 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1656850520, at line 897 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Line	1004	1004
Object	Namespace1656850520	Namespace1656850520

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1004.     (void)
memset(cin.file.create_time,0,sizeof(cin.file.create_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=39

Status	New

The size of the buffer used by WriteCINImage in Namespace1656850520, at line 897 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1656850520, at line 897 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Line	1098	1098
Object	Namespace1656850520	Namespace1656850520

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1098.       sizeof(cin.origination.create_date));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=40
Status	New

The size of the buffer used by WriteCINImage in Namespace1656850520, at line 897 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1656850520, at line 897 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Line	1103	1103
Object	Namespace1656850520	Namespace1656850520

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1103.       sizeof(cin.origination.create_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=41
Status	New

The size of the buffer used by *ReadCINImage in Namespace1656850520, at line 380 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadCINImage passes to Namespace1656850520, at line 380 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Line	626	626
Object	Namespace1656850520	Namespace1656850520

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-28463-FP.c
Method static Image *ReadCINImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
626.      sizeof(cin.origination.serial));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=42
Status	New

The size of the buffer used by WriteCINImage in Namespace1291186819, at line 897 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1291186819, at line 897 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Line	1000	1000
Object	Namespace1291186819	Namespace1291186819

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1000.     (void)
memset(cin.file.create_date,0,sizeof(cin.file.create_date));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=43
Status	New

The size of the buffer used by WriteCINImage in Namespace1291186819, at line 897 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1291186819, at line 897 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Line	1004	1004
Object	Namespace1291186819	Namespace1291186819

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c

Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1004.     (void)
memset(cin.file.create_time,0,sizeof(cin.file.create_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=44
Status	New

The size of the buffer used by WriteCINImage in Namespace1291186819, at line 897 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1291186819, at line 897 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Line	1098	1098

Object	Namespace1291186819	Namespace1291186819

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1098.      sizeof(cin.origination.create_date));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=45
Status	New

The size of the buffer used by WriteCINImage in Namespace1291186819, at line 897 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WriteCINImage passes to Namespace1291186819, at line 897 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Line	1103	1103
Object	Namespace1291186819	Namespace1291186819

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Method static MagickBooleanType WriteCINImage(const ImageInfo *image_info,Image *image,

```
....
1103.       sizeof(cin.origination.create_time));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=46
Status	New

The size of the buffer used by *ReadCINImage in Namespace1291186819, at line 380 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadCINImage passes to Namespace1291186819, at line 380 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Line	626	626
Object	Namespace1291186819	Namespace1291186819

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-28463-FP.c
Method static Image *ReadCINImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
626.      sizeof(cin.origination.serial));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=47
Status	New

The size of the buffer used by WritePCLImage in length, at line 657 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WritePCLImage passes to length, at line 657 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Line	951	951
Object	length	length

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image,

```
....
951.            (void) memcpy(previous_pixels,pixels,length*
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=48
Status	New

The size of the buffer used by WritePCLImage in pixels, at line 657 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WritePCLImage passes to pixels, at line 657 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Line	952	952
Object	pixels	pixels

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image,

```
....
952.              sizeof(*pixels));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=49
Status New

The size of the buffer used by WritePCLImage in length, at line 657 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WritePCLImage passes to length, at line 657 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Line	951	951
Object	length	length

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image,

```
....
951.            (void) memcpy(previous_pixels,pixels,length*
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10

	028&pathid=50
Status	New

The size of the buffer used by WritePCLImage in pixels, at line 657 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WritePCLImage passes to pixels, at line 657 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Line	952	952
Object	pixels	pixels

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image,

```
....
952.              sizeof(*pixels));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=51
Status	New

The size of the buffer used by deshufflePalette in image, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to image, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Line	219	219
Object	image	image

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
219.    (void) memcpy(oldColormap,image->colormap,(size_t)image->colors*
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=52
Status	New

The size of the buffer used by deshufflePalette in oldColormap, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to oldColormap, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Line	220	220
Object	oldColormap	oldColormap

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
220.      sizeof(*oldColormap));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=53
Status	New

The size of the buffer used by deshufflePalette in colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Line	227	227
Object	colors	colors

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
227.      memcpy(&(image-
>colormap[i+1*colors]),&(oldColormap[i+2*colors]),colors*
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=54
Status	New

The size of the buffer used by deshufflePalette in PixelInfo, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to PixelInfo, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Line	228	228
Object	PixelInfo	PixelInfo

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
228.         sizeof(PixelInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=55
Status	New

The size of the buffer used by deshufflePalette in colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Line	229	229
Object	colors	colors

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
229.       memcpy(&(image-
>colormap[i+2*colors]),&(oldColormap[i+1*colors]),colors*
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=56
Status	New

The size of the buffer used by deshufflePalette in PixelInfo, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to PixelInfo, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Line	230	230
Object	PixelInfo	PixelInfo

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c

Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
230.         sizeof(PixelInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=57
Status	New

The size of the buffer used by deshufflePalette in image, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to image, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Line	219	219
Object	image	image

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c

Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
219.    (void) memcpy(oldColormap,image->colormap,(size_t)image->colors*
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=58
Status	New

The size of the buffer used by deshufflePalette in oldColormap, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to oldColormap, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Line	220	220
Object	oldColormap	oldColormap

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
220.      sizeof(*oldColormap));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=59
Status	New

The size of the buffer used by deshufflePalette in colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Line	227	227
Object	colors	colors

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c

Method	static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
227.      memcpy(&(image-
>colormap[i+1*colors]),&(oldColormap[i+2*colors]),colors*
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=60
Status	New

The size of the buffer used by deshufflePalette in PixelInfo, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to PixelInfo, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Line	228	228
Object	PixelInfo	PixelInfo

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Method	static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
228.        sizeof(PixelInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=61
Status	New

The size of the buffer used by deshufflePalette in colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Line	229	229
Object	colors	colors

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
229.      memcpy(&(image-
>colormap[i+2*colors]),&(oldColormap[i+1*colors]),colors*
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=62
Status	New

The size of the buffer used by deshufflePalette in PixelInfo, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to PixelInfo, at line 206 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Line	230	230
Object	PixelInfo	PixelInfo

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
230.        sizeof(PixelInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=63
Status	New

The size of the buffer used by WritePCLImage in length, at line 666 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WritePCLImage passes to length, at line 666 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Line	960	960

Object	length	length

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image,

```
....
960.            (void) memcpy(previous_pixels,pixels,length*
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=64
Status New

The size of the buffer used by WritePCLImage in pixels, at line 666 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WritePCLImage passes to pixels, at line 666 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Line	961	961
Object	pixels	pixels

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image,

```
....
961.              sizeof(*pixels));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=65
Status New

The size of the buffer used by deshufflePalette in image, at line 206 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to image, at line 206 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination

File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Line	219	219
Object	image	image

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
219.     (void) memcpy(oldColormap,image->colormap,(size_t)image->colors*
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=66
Status	New

The size of the buffer used by deshufflePalette in oldColormap, at line 206 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to oldColormap, at line 206 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Line	220	220
Object	oldColormap	oldColormap

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
220.       sizeof(*oldColormap));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=67
Status	New

The size of the buffer used by deshufflePalette in colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Line	227	227
Object	colors	colors

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
227.      memcpy(&(image-
>colormap[i+1*colors]),&(oldColormap[i+2*colors]),colors*
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=68
Status	New

The size of the buffer used by deshufflePalette in PixelInfo, at line 206 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that deshufflePalette passes to PixelInfo, at line 206 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Line	228	228
Object	PixelInfo	PixelInfo

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
228.        sizeof(PixelInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=69
Status	New

The size of the buffer used by deshufflePalette in colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that deshufflePalette passes to colors, at line 206 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Line	229	229
Object	colors	colors

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
229.      memcpy(&(image-
>colormap[i+2*colors]),&(oldColormap[i+1*colors]),colors*
```

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=1010039&projectid=10028&pathid=258
Status	New

The dangerous function, memcpy, was found in use at line 657 in ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Line	951	951
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image,

```
....
951.            (void) memcpy(previous_pixels,pixels,length*
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=259
Status	New

The dangerous function, memcpy, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Line	3238	3238
Object	memcpy	memcpy

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c

Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3238.            memcpy(&info,info_copy,sizeof(info));
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=260
Status	New

The dangerous function, memcpy, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Line	3249	3249
Object	memcpy	memcpy

Code Snippet

File Name	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3249.            memcpy(info_copy,&info,sizeof(info));
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=261
Status	New

The dangerous function, memcpy, was found in use at line 657 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Line	951	951
Object	memcpy	memcpy

Code Snippet

File Name	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Method	static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image,

```
....
951.            (void) memcpy(previous_pixels,pixels,length*
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=262
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Line	219	219

Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
219.     (void) memcpy(oldColormap,image->colormap,(size_t)image->colors*
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=263
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Line	227	227
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
227.       memcpy(&(image-
>colormap[i+1*colors]),&(oldColormap[i+2*colors]),colors*
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=264
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c

Line	229	229
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
229.      memcpy(&(image-
>colormap[i+2*colors]),&(oldColormap[i+1*colors]),colors*
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=265
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Line	219	219
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
219.    (void) memcpy(oldColormap,image->colormap,(size_t)image->colors*
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=266
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Line	227	227
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
227.      memcpy(&(image-
>colormap[i+1*colors]),&(oldColormap[i+2*colors]),colors*
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=267
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Line	229	229
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
229.      memcpy(&(image-
>colormap[i+2*colors]),&(oldColormap[i+1*colors]),colors*
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=268
Status	New

The dangerous function, memcpy, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	3238	3238
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3238.            memcpy(&info,info_copy,sizeof(info));
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=269
Status	New

The dangerous function, memcpy, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	3249	3249
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3249.            memcpy(info_copy,&info,sizeof(info));
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=270
Status	New

The dangerous function, memcpy, was found in use at line 666 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Line	960	960
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image,

```
....
960.            (void) memcpy(previous_pixels,pixels,length*
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=271
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Line	219	219
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
219.    (void) memcpy(oldColormap,image->colormap,(size_t)image->colors*
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=272

Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Line	227	227
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
227.      memcpy(&(image-
>colormap[i+1*colors]),&(oldColormap[i+2*colors]),colors*
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=273
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Line	229	229
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
229.      memcpy(&(image-
>colormap[i+2*colors]),&(oldColormap[i+1*colors]),colors*
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=274
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c
Line	219	219
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
219.     (void) memcpy(oldColormap,image->colormap,(size_t)image->colors*
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=275
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c
Line	227	227
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
227.       memcpy(&(image-
>colormap[i+1*colors]),&(oldColormap[i+2*colors]),colors*
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=276
Status	New

The dangerous function, memcpy, was found in use at line 206 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c
Line	229	229
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
229.      memcpy(&(image-
>colormap[i+2*colors]),&(oldColormap[i+1*colors]),colors*
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=277
Status	New

The dangerous function, memcpy, was found in use at line 657 in ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Line	951	951
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image,

```
....
951.            (void) memcpy(previous_pixels,pixels,length*
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=278
Status	New

The dangerous function, memcpy, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	3240	3240
Object	memcpy	memcpy

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c

Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3240.            memcpy(&info,info_copy,sizeof(info));
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=279
Status	New

The dangerous function, memcpy, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	3251	3251
Object	memcpy	memcpy

Code Snippet

File Name	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3251.            memcpy(info_copy,&info,sizeof(info));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=280
Status	New

The dangerous function, memcpy, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	3240	3240
Object	memcpy	memcpy

Code Snippet

File Name	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3240.            memcpy(&info,info_copy,sizeof(info));
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=281
Status	New

The dangerous function, memcpy, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	3251	3251

Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3251.            memcpy(info_copy,&info,sizeof(info));
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=282
Status	New

The dangerous function, sscanf, was found in use at line 3001 in ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Line	3377	3377
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3377.                        count=(ssize_t)
sscanf(transfer_syntax+17,".%d.%d",&type,
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=283
Status	New

The dangerous function, sscanf, was found in use at line 251 in ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-0284-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-0284-TP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-0284-TP.c
Line	347	347
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-0284-TP.c
Method static Image *ReadXPMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
347.      count=(ssize_t) sscanf(p+1,"%lu %lu %lu
%lu",&columns,&rows,&colors,&width);
```

Dangerous Functions\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=284
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Line	275	275
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
275.          count=(ssize_t) sscanf(command,"CropBox [%lf %lf %lf %lf",
```

Dangerous Functions\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=285
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Line	278	278
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
278.            count=(ssize_t) sscanf(command,"CropBox[%lf %lf %lf
%lf",
```

Dangerous Functions\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=286
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Line	286	286
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
286.          count=(ssize_t) sscanf(command,"MediaBox [%lf %lf %lf
%lf",
```

Dangerous Functions\Path 30:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=287
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Line	289	289
Object	sscanf	sscanf

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c

Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
289.            count=(ssize_t) sscanf(command,"MediaBox[%lf %lf %lf
%lf",
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=288
Status	New

The dangerous function, sscanf, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Line	3419	3419
Object	sscanf	sscanf

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c

Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3419.                          count=(ssize_t)
sscanf(transfer_syntax+17,".%d.%d",&type,
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=289
Status	New

The dangerous function, sscanf, was found in use at line 251 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-0284-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-0284-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-0284-TP.c
Line	347	347
Object	sscanf	sscanf

Code Snippet

File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-0284-TP.c

Method static Image *ReadXPMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
347.      count=(ssize_t) sscanf(p+1,"%lu %lu %lu
%lu",&columns,&rows,&colors,&width);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=290
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Line	275	275
Object	sscanf	sscanf

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Method	static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
275.          count=(ssize_t) sscanf(command,"CropBox [%lf %lf %lf %lf",
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=291
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Line	278	278
Object	sscanf	sscanf

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Method	static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
278.            count=(ssize_t) sscanf(command,"CropBox[%lf %lf %lf
%lf",
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=292
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-	ImageMagick@@ImageMagick-7.0.10-

	36-CVE-2022-32546-TP.c	36-CVE-2022-32546-TP.c
Line	286	286
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
286.          count=(ssize_t) sscanf(command,"MediaBox [%lf %lf %lf
%lf",
```

Dangerous Functions\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=293
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Line	289	289
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
289.           count=(ssize_t) sscanf(command,"MediaBox[%lf %lf %lf
%lf",
```

Dangerous Functions\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=294
Status New

The dangerous function, sscanf, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	3420	3420
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3420.                          count=(ssize_t)
sscanf(transfer_syntax+17,".%d.%d",&type,
```

Dangerous Functions\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=295
Status New

The dangerous function, sscanf, was found in use at line 251 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-0284-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-0284-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-0284-TP.c
Line	347	347
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-0284-TP.c
Method static Image *ReadXPMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
347.      count=(ssize_t) sscanf(p+1,"%lu %lu %lu
%lu",&columns,&rows,&colors,&width);
```

Dangerous Functions\Path 39:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=296
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Line	275	275
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
275.          count=(ssize_t) sscanf(command,"CropBox [%lf %lf %lf %lf",
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=297
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Line	278	278
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
278.            count=(ssize_t) sscanf(command,"CropBox[%lf %lf %lf
%lf",
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=298
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Line	286	286
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
286.          count=(ssize_t) sscanf(command,"MediaBox [%lf %lf %lf
%lf",
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=299
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Line	289	289
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
289.            count=(ssize_t) sscanf(command,"MediaBox[%lf %lf %lf
%lf",
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=300
Status	New

The dangerous function, sscanf, was found in use at line 3001 in ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Line	3377	3377
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3377.                        count=(ssize_t)
sscanf(transfer_syntax+17,".%d.%d",&type,
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=301
Status	New

The dangerous function, sscanf, was found in use at line 249 in ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-0284-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-0284-TP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-0284-TP.c
Line	345	345
Object	sscanf	sscanf

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-0284-TP.c
Method	static Image *ReadXPMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
345.      count=(ssize_t) sscanf(p+1,"%lu %lu %lu
%lu",&columns,&rows,&colors,&width);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=302
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Line	275	275
Object	sscanf	sscanf

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Method	static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
275.          count=(ssize_t) sscanf(command,"CropBox [%lf %lf %lf %lf",
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=303
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-	ImageMagick@@ImageMagick-7.0.10-7-

	CVE-2022-32546-TP.c	CVE-2022-32546-TP.c
Line	278	278
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
278.            count=(ssize_t) sscanf(command,"CropBox[%lf %lf %lf
%lf",
```

Dangerous Functions\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=304
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Line	286	286
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
286.          count=(ssize_t) sscanf(command,"MediaBox [%lf %lf %lf
%lf",
```

Dangerous Functions\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=305
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Line	289	289
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Method static Image *ReadPCLImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
289.            count=(ssize_t) sscanf(command,"MediaBox[%lf %lf %lf
%lf",
```

Dangerous Functions\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=306
Status New

The dangerous function, sscanf, was found in use at line 3003 in ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	3422	3422
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3422.                        count=(ssize_t)
sscanf(transfer_syntax+17,".%d.%d",&type,
```

Dangerous Functions\Path 50:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=307
Status	New

The dangerous function, sscanf, was found in use at line 251 in ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-0284-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-0284-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-0284-TP.c
Line	347	347
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-0284-TP.c
Method static Image *ReadXPMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
347.      count=(ssize_t) sscanf(p+1,"%lu %lu %lu
%lu",&columns,&rows,&colors,&width);
```

Integer Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Integer Overflow Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description
Integer Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=222
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2828 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Line	2912	2912
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2912.                index=(int) scaled_value;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=223
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2828 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Line	2929	2929
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2929.                        index=(int) (info-
>max_value*(((scaled_value-
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=224
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2830 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Line	2914	2914
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2914.                index=(int) scaled_value;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=225
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2830 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Line	2931	2931
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2931.                        index=(int) (info-
>max_value*(((scaled_value-
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=226
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2830 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	2914	2914
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2914.                index=(int) scaled_value;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=227
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2830 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	2931	2931
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2931.                        index=(int) (info-
>max_value*(((scaled_value-
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=228
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2828 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Line	2912	2912
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2912.                index=(int) scaled_value;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=229
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2828 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Line	2929	2929
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2929.                        index=(int) (info-
>max_value*(((scaled_value-
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=230
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2830 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	2914	2914
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2914.                index=(int) scaled_value;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=231
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2830 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	2931	2931
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2931.                        index=(int) (info-
>max_value*(((scaled_value-
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=232
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2830 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	2914	2914
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2914.                index=(int) scaled_value;
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=233
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2830 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	2931	2931
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Method	static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2931.                        index=(int) (info-
>max_value*(((scaled_value-
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=234
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3001 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Line	3577	3577
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3577.                datum=(int) colors;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=235
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3001 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Line	3604	3604
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3604.                datum=(int) colors;
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=236
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3001 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Line	3636	3636

Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3636.                datum=(int) colors;
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=237
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3001 of ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Line	3668	3668
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3668.                datum=(int) colors;
```

Integer Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=238
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c

Line	3619	3619
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3619.                datum=(int) colors;
```

Integer Overflow\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=239
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Line	3646	3646
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3646.                datum=(int) colors;
```

Integer Overflow\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=240
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-	ImageMagick@@ImageMagick-7.0.10-

	36-CVE-2021-3962-FP.c	36-CVE-2021-3962-FP.c
Line	3678	3678
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3678.                datum=(int) colors;
```

Integer Overflow\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=241
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Line	3710	3710
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3710.                datum=(int) colors;
```

Integer Overflow\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=242
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	3620	3620
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3620.                datum=(int) colors;
```

Integer Overflow\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=243
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	3647	3647
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3647.                datum=(int) colors;
```

Integer Overflow\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=244
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	3679	3679
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3679.                datum=(int) colors;
```

Integer Overflow\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=245
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	3711	3711
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3711.                datum=(int) colors;
```

Integer Overflow\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=246
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3001 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Line	3577	3577
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3577.                datum=(int) colors;
```

Integer Overflow\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=247
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3001 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Line	3604	3604
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3604.                datum=(int) colors;
```

Integer Overflow\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=248
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3001 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Line	3636	3636
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3636.                datum=(int) colors;
```

Integer Overflow\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=249
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3001 of ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Line	3668	3668
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3668.                datum=(int) colors;
```

Integer Overflow\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=250

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	3622	3622
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3622.                datum=(int) colors;
```

Integer Overflow\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=251
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	3649	3649
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3649.                datum=(int) colors;
```

Integer Overflow\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10

	028&pathid=252
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	3681	3681
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3681.                datum=(int) colors;
```

Integer Overflow\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=253
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	3713	3713
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3713.                datum=(int) colors;
```

Integer Overflow\Path 33:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=254
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	3622	3622
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3622.                datum=(int) colors;
```

Integer Overflow\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=255
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	3649	3649
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3649.                datum=(int) colors;
```

Integer Overflow\Path 35:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=256
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	3681	3681
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3681.                datum=(int) colors;
```

Integer Overflow\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=257
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3003 of ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	3713	3713
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3713.                datum=(int) colors;
```

Memory Leak

Query Path:

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=1010039&projectid=10028&pathid=348
Status	New

	Source	Destination
File	hpjansson@@chafa-1.10.0-CVE-2022-2061-TP.c	hpjansson@@chafa-1.10.0-CVE-2022-2061-TP.c
Line	91	91
Object	c	c

Code Snippet
File Name hpjansson@@chafa-1.10.0-CVE-2022-2061-TP.c
Method lzw_result lzw_context_create(struct lzw_ctx **ctx)

```
....
91.   struct lzw_ctx *c = malloc(sizeof(*c));
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=349
Status	New

	Source	Destination
File	hpjansson@@chafa-1.4.0-CVE-2022-2061-TP.c	hpjansson@@chafa-1.4.0-CVE-2022-2061-TP.c
Line	91	91
Object	c	c

Code Snippet
File Name hpjansson@@chafa-1.4.0-CVE-2022-2061-TP.c
Method lzw_result lzw_context_create(struct lzw_ctx **ctx)

```
....
91.   struct lzw_ctx *c = malloc(sizeof(*c));
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=350
Status	New

	Source	Destination
File	hpjansson@@chafa-1.6.0-CVE-2022-2061-TP.c	hpjansson@@chafa-1.6.0-CVE-2022-2061-TP.c
Line	91	91
Object	c	c

Code Snippet
File Name hpjansson@@chafa-1.6.0-CVE-2022-2061-TP.c
Method lzw_result lzw_context_create(struct lzw_ctx **ctx)

```
....
91.   struct lzw_ctx *c = malloc(sizeof(*c));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=351
Status	New

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	806	806
Object	data	data

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method BN_to_integer(krb5_context context, BIGNUM *bn, heim_integer *integer)

```
....
806.      integer->data = malloc(integer->length);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=352
Status	New

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1821	1821
Object	subject	subject

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method add_principal_mapping(krb5_context context,

```
....
1821.     principal_mappings.val[principal_mappings.len].subject =
strdup(subject);
```

Memory Leak\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=353
Status New

	Source	Destination
File	hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c	hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c
Line	1034	1034
Object	local_colour_table	local_colour_table

Code Snippet
File Name hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c
Method gif_result gif_initialise(gif_animation *gif, size_t size, unsigned char *data)

```
....
1034.                   gif->local_colour_table = calloc(GIF_MAX_COLOURS,
sizeof(unsigned int));
```

Memory Leak\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=354
Status New

	Source	Destination
File	hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c	hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c

Line	1059	1059
Object	frames	frames

Code Snippet
File Name hpjansson@@chafa-1.10.0-CVE-2022-1507-TP.c
Method gif_result gif_initialise(gif_animation *gif, size_t size, unsigned char *data)

```
....
1059.                   if ((gif->frames = (gif_frame
*)malloc(sizeof(gif_frame))) == NULL) {
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=355
Status New

	Source	Destination
File	hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c	hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c
Line	1035	1035
Object	local_colour_table	local_colour_table

Code Snippet
File Name hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c
Method gif_result gif_initialise(gif_animation *gif, size_t size, unsigned char *data)

```
....
1035.                   gif->local_colour_table = calloc(GIF_MAX_COLOURS,
sizeof(unsigned int));
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=356
Status New

	Source	Destination
File	hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c	hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c
Line	1060	1060
Object	frames	frames

Code Snippet

File Name	hpjansson@@chafa-1.4.0-CVE-2022-1507-TP.c
Method	gif_result gif_initialise(gif_animation *gif, size_t size, unsigned char *data)

```
....
1060.                   if ((gif->frames = (gif_frame
*)malloc(sizeof(gif_frame))) == NULL) {
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=357
Status	New

	Source	Destination
File	hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c	hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c
Line	1035	1035
Object	local_colour_table	local_colour_table

Code Snippet

File Name	hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c
Method	gif_result gif_initialise(gif_animation *gif, size_t size, unsigned char *data)

```
....
1035.                   gif->local_colour_table = calloc(GIF_MAX_COLOURS,
sizeof(unsigned int));
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=358
Status	New

	Source	Destination
File	hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c	hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c
Line	1060	1060
Object	frames	frames

Code Snippet

File Name	hpjansson@@chafa-1.6.0-CVE-2022-1507-TP.c
Method	gif_result gif_initialise(gif_animation *gif, size_t size, unsigned char *data)

```
....
1060.                   if ((gif->frames = (gif_frame
*)malloc(sizeof(gif_frame))) == NULL) {
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=359
Status	New

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1682	1682
Object	subject_name	subject_name

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method _kdc_pk_check_client(krb5_context context,

```
....
1682.       *subject_name = strdup("<unauthenticated anonymous
client>");
```

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=1010039&projectid=10028&pathid=213
Status	New

Calling free() (line 1912) on a variable that was not dynamically allocated (line 1912) in file heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c may result with a crash.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1979	1979
Object	str	str

Code Snippet

File Name	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method	krb5_kdc_pk_initialize(krb5_context context,

```
....
1979.                   free(str);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=214
Status	New

Calling free() (line 1912) on a variable that was not dynamically allocated (line 1912) in file heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c may result with a crash.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	2015	2015
Object	fn	fn

Code Snippet

File Name	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method	krb5_kdc_pk_initialize(krb5_context context,

```
....
2015.       free(fn);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=215
Status	New

Calling free() (line 110) on a variable that was not dynamically allocated (line 110) in file heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c may result with a crash.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	144	144
Object	buf	buf

Code Snippet

File Name	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c

Method	pk_check_pkauthenticator(krb5_context context,

```
....
144.        free(buf);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=216
Status	New

Calling free() (line 1125) on a variable that was not dynamically allocated (line 1125) in file heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c may result with a crash.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1316	1316
Object	kckdata	kckdata

Code Snippet	
File Name	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method	_kdc_pk_mk_pa_reply(krb5_context context,

```
....
1316.              free(kckdata);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=217
Status	New

Calling free() (line 1125) on a variable that was not dynamically allocated (line 1125) in file heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c may result with a crash.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1336	1336
Object	buf	buf

Code Snippet	
File Name	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method	_kdc_pk_mk_pa_reply(krb5_context context,

```
....
1336.                   free(buf);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=218
Status	New

Calling free() (line 1125) on a variable that was not dynamically allocated (line 1125) in file heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c may result with a crash.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1429	1429
Object	buf	buf

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1429.            free(buf);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=219
Status	New

Calling free() (line 1125) on a variable that was not dynamically allocated (line 1125) in file heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c may result with a crash.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1441	1441
Object	buf	buf

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1441.       free(buf);
```

Use After Free

Query Path:
CPP\Cx\CPP Medium Threat\Use After Free Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Use After Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=360
Status	New

The pointer kckdata at heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c in line 1125 is being used after it has been freed.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1316	1314
Object	kckdata	kckdata

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1316.           free(kckdata);
....
1314.                                   kckdata, kcklen, 0, &kx);
```

Use After Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=361
Status	New

The pointer buf at heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c in line 1125 is being used after it has been freed.

	Source	Destination

File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1336	1353
Object	buf	buf

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1336.                   free(buf);
....
1353.           ASN1_MALLOC_ENCODE(PA_PK_AS_REP_BTMM, buf, len, &btmm,
&size, ret);
```

Use After Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=362
Status	New

The pointer buf at heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c in line 1125 is being used after it has been freed.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1336	1355
Object	buf	buf

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1336.                   free(buf);
....
1355.           ASN1_MALLOC_ENCODE(PA_PK_AS_REP, buf, len, &rep, &size,
ret);
```

Wrong Size t Allocation

Query Path:
CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0

Description

Wrong Size t Allocation\Path 1:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=220
Status	New

The function size in heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c at line 197 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	225	225
Object	size	size

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method generate_dh_keyblock(krb5_context context,

```
....
225.        dh_gen_key = malloc(size);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=221
Status	New

The function tmp_len in heimdal@@heimdal-heimdal-7.7.1-CVE-2022-41916-FP.c at line 297 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2022-41916-FP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2022-41916-FP.c
Line	312	312
Object	tmp_len	tmp_len

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2022-41916-FP.c
Method _wind_stringprep_normalize(const uint32_t *in, size_t in_len,

```
....
312.      tmp = malloc(tmp_len * sizeof(uint32_t));
```

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=1010039&projectid=10028&pathid=363
Status	New

The variable declared in principal at heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c in line 1592 is not initialized when it is used by principal at heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c in line 1592.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1600	1649
Object	principal	principal

Code Snippet

File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c

Method match_ms_upn_san(krb5_context context,

```
....
1600.       krb5_principal principal = NULL;
....
1649.        strupr(principal->realm);
```

Potential Off by One Error in Loops

Query Path:

CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=10
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c at line 3001 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Line	3958	3958
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3958.          for (i=0; i <= (ssize_t) GetQuantumRange(info.depth);
i++)
```

Potential Off by One Error in Loops\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=11
Status New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c at line 556 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Line	646	646
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
646.          for (j=0; j <= (ssize_t) count; j++)
```

Potential Off by One Error in Loops\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=12
Status New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c at line 3003 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Line	4002	4002
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
4002.          for (i=0; i <= (ssize_t) GetQuantumRange(info.depth);
i++)
```

Potential Off by One Error in Loops\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=13
Status New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c at line 556 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Line	646	646
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
646.          for (j=0; j <= (ssize_t) count; j++)
```

Potential Off by One Error in Loops\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=14
Status New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c at line 3003 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	4003	4003
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
4003.          for (i=0; i <= (ssize_t) GetQuantumRange(info.depth);
i++)
```

Potential Off by One Error in Loops\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=15
Status New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c at line 565 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Line	655	655
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
655.          for (j=0; j <= (ssize_t) count; j++)
```

Potential Off by One Error in Loops\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=16
Status New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c at line 3001 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Line	3958	3958
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3958.          for (i=0; i <= (ssize_t) GetQuantumRange(info.depth);
i++)
```

Potential Off by One Error in Loops\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=17
Status New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c at line 556 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Line	646	646
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-7-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
646.          for (j=0; j <= (ssize_t) count; j++)
```

Potential Off by One Error in Loops\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=18
Status New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c at line 3003 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	4007	4007
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
4007.          for (i=0; i <= (ssize_t) GetQuantumRange(info.depth);
i++)
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=19
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c at line 3003 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	4007	4007
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
4007.          for (i=0; i <= (ssize_t) GetQuantumRange(info.depth);
i++)
```

Improper Resource Access Authorization

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=364
Status	New

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1876	1876
Object	fgets	fgets

Code Snippet

File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c

Method load_mappings(krb5_context context, const char *fn)

```
....
1876.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=365
Status	New

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1876	1876
Object	buf	buf

Code Snippet

File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c

Method load_mappings(krb5_context context, const char *fn)

```
....
1876.       while (fgets(buf, sizeof(buf), f) != NULL) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10

	028&pathid=366
Status	New

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1479	1479
Object	data	data

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1479.           ret = read(fd, ocsp.data.data, sb.st_size);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=367
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Line	3894	3894
Object	fputc	fputc

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-25-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3894.               if (fputc(c,file) != c)
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=368
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-	ImageMagick@@ImageMagick-7.0.10-

	36-CVE-2021-3962-FP.c	36-CVE-2021-3962-FP.c
Line	3938	3938
Object	fputc	fputc

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-36-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3938.               if (fputc(c,file) != c)
```

Improper Resource Access Authorization\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=369
Status New

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Line	3939	3939
Object	fputc	fputc

Code Snippet
File Name ImageMagick@@ImageMagick-7.0.10-62-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3939.               if (fputc(c,file) != c)
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=370
Status New

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Line	3894	3894
Object	fputc	fputc

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.10-7-CVE-2021-3962-FP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3894.              if (fputc(c,file) != c)
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=371
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Line	3941	3941
Object	fputc	fputc

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.11-12-CVE-2021-3962-FP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3941.              if (fputc(c,file) != c)
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=372
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Line	3941	3941
Object	fputc	fputc

Code Snippet	
File Name	ImageMagick@@ImageMagick-7.0.11-12-CVE-2022-1114-TP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3941.              if (fputc(c,file) != c)
```

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=1010039&projectid=10028&pathid=374
Status	New

The _kdc_pk_check_client method calls the Pointer function, at line 1664 of heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1682	1682
Object	Pointer	Pointer

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method _kdc_pk_check_client(krb5_context context,

```
....
1682.       *subject_name = strdup("<unauthenticated anonymous
client>");
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=375
Status	New

The add_principal_mapping method calls the subject function, at line 1801 of heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1821	1821
Object	subject	subject

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method add_principal_mapping(krb5_context context,

```
....
1821.     principal_mappings.val[principal_mappings.len].subject =
strdup(subject);
```

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=1010039&projectid=10028&pathid=378
Status	New

The load_mappings method in heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1872	1872
Object	fopen	fopen

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1872.      f = fopen(fn, "r");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=379
Status	New

The _kdc_pk_mk_pa_reply method in heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1456	1456
Object	open	open

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method _kdc_pk_mk_pa_reply(krb5_context context,

```
....
1456.           fd = open(config->pkinit_kdc_ocsp_file, O_RDONLY);
```

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=1010039&projectid=10028&pathid=373
Status New

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1872	1872
Object	f	f

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method load_mappings(krb5_context context, const char *fn)

```
....
1872.       f = fopen(fn, "r");
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description
NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=376
Status	New

The variable declared in null at heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c in line 1592 is not initialized when it is used by principal at heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c in line 1592.

	Source	Destination
File	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Line	1600	1649
Object	null	principal

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2023-5568-TP.c
Method match_ms_upn_san(krb5_context context,

```
....
1600.       krb5_principal principal = NULL;
....
1649.        strupr(principal->realm);
```

Unchecked Array Index

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description
Unchecked Array Index\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1010039&projectid=10028&pathid=377
Status	New

	Source	Destination

File	heimdal@@heimdal-heimdal-7.7.1-CVE-2022-41916-FP.c	heimdal@@heimdal-heimdal-7.7.1-CVE-2022-41916-FP.c
Line	279	279
Object	ostarter	ostarter

Code Snippet
File Name heimdal@@heimdal-heimdal-7.7.1-CVE-2022-41916-FP.c
Method combine(const uint32_t *in, size_t in_len,

```
....
279.                    out[ostarter] = comb;
```

Buffer Overflow boundedcpy

Risk

What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

Cause

How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

General Recommendations

How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

Source Code Examples

CPP

Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

```
```

Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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

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));
    }
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

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 After Free

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
//..
```

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());
```

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

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

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

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