vul_files_28 Scan Report

Project Name	vul_files_28
Scan Start	Tuesday, January 7, 2025 2:45:15 PM
Preset	Checkmarx Default
Scan Time	02h:45m:12s
Lines Of Code Scanned	297603
Files Scanned	75
Report Creation Time	Tuesday, January 7, 2025 5:25:38 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030
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

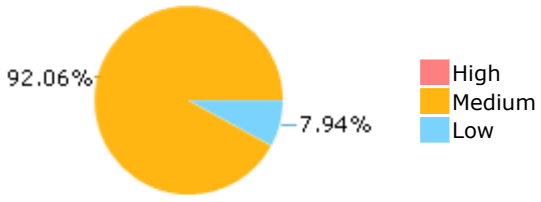
Results Limit

Results limit per query was set to 50

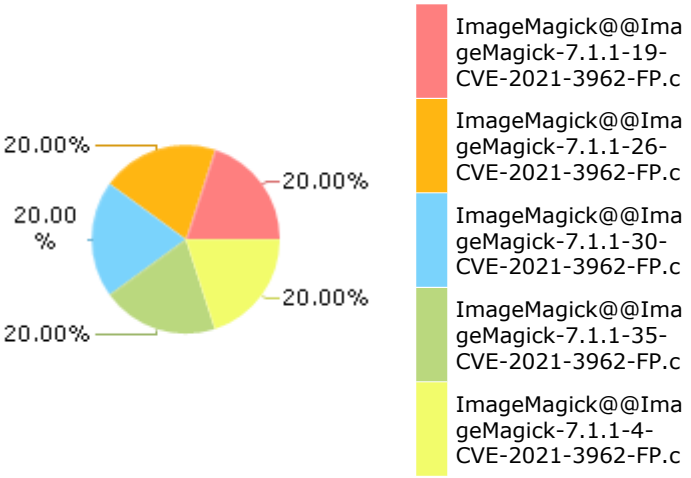
Selected Queries

Selected queries are listed in Result Summary

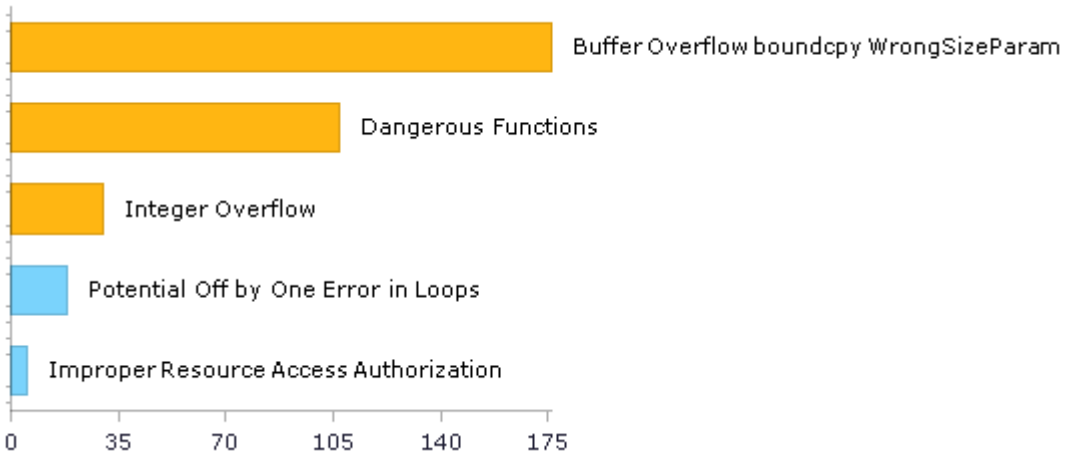
Result Summary



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	194	194
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	9	9
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	107	107
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	107	107
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	18	18
PCI DSS (3.2) - 6.5.2 - Buffer overflows	206	206
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.	4	4
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.	5	5
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.	30	30

***** 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)	9	9
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)*	0	0
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	30	30
SI-11 Error Handling (P2)*	0	0
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	18	18

***** 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

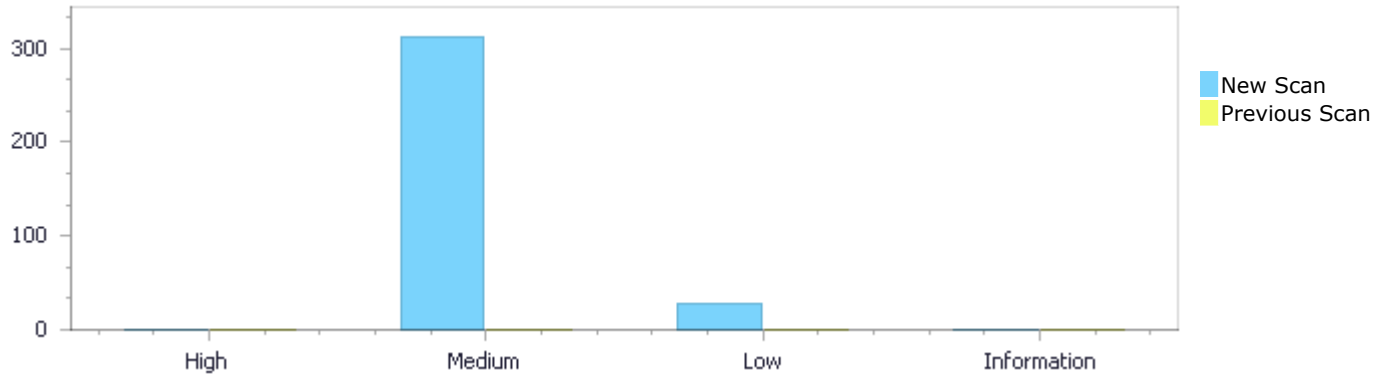
Scan Summary - Custom

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	0	313	27	0	340
Recurrent Issues	0	0	0	0	0
Total	0	313	27	0	340
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	0	313	27	0	340
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	313	27	0	340

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow boundcpy WrongSizeParam	176	Medium
Dangerous Functions	107	Medium
Integer Overflow	30	Medium
Potential Off by One Error in Loops	18	Low
Improper Resource Access Authorization	5	Low

Incorrect Permission Assignment For Critical Resources	4	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c	25
ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c	25
ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c	25
ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c	25
ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c	25
ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c	18
ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c	18
ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c	18
ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c	18
ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c	18

Scan Results Details

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=1020037&projectid=20030&pathid=19
Status	New

The size of the buffer used by *ReadDCMImage in info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-19-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 3048 of ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	3271	3271
Object	info	info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3271.            (void) memcpy(clone_info,&info,sizeof(info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=20
Status	New

The size of the buffer used by *ReadDCMImage in info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-26-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 3048 of ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3271	3271
Object	info	info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3271.            (void) memcpy(clone_info,&info,sizeof(info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=21
Status New

The size of the buffer used by *ReadDCMImage in info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-30-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 3048 of ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3271	3271
Object	info	info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3271.            (void) memcpy(clone_info,&info,sizeof(info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=22
Status New

The size of the buffer used by *ReadDCMImage in info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-35-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 3048 of ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3271	3271
Object	info	info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3271.            (void) memcpy(clone_info,&info,sizeof(info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=23
Status New

The size of the buffer used by *ReadDCMImage in info, at line 3052 of ImageMagick@@ImageMagick-7.1.1-4-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 3052 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	3277	3277
Object	info	info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3277.            (void) memcpy(clone_info,&info,sizeof(info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20

	030&pathid=24
Status	New

The size of the buffer used by *ReadEMFImage in BITMAPINFO, at line 439 of ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadEMFImage passes to BITMAPINFO, at line 439 of ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c
Line	569	569
Object	BITMAPINFO	BITMAPINFO

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c
Method static Image *ReadEMFImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
569.     (void) memset(&DIBinfo,0,sizeof(BITMAPINFO));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=25
Status	New

The size of the buffer used by *ReadEMFImage in BITMAPINFO, at line 439 of ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadEMFImage passes to BITMAPINFO, at line 439 of ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c
Line	569	569
Object	BITMAPINFO	BITMAPINFO

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c
Method static Image *ReadEMFImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
569.     (void) memset(&DIBinfo,0,sizeof(BITMAPINFO));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=26
Status	New

The size of the buffer used by *ReadEMFImage in BITMAPINFO, at line 439 of ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadEMFImage passes to BITMAPINFO, at line 439 of ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c
Line	569	569
Object	BITMAPINFO	BITMAPINFO

Code Snippet

File Name ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c

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

```
....
569.     (void) memset(&DIBinfo,0,sizeof(BITMAPINFO));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=27
Status	New

The size of the buffer used by *ReadEMFImage in BITMAPINFO, at line 439 of ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ReadEMFImage passes to BITMAPINFO, at line 439 of ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c
Line	569	569
Object	BITMAPINFO	BITMAPINFO

Code Snippet

File Name ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c

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

```
....
569.    (void) memset(&DIBinfo,0,sizeof(BITMAPINFO));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=28
Status	New

The size of the buffer used by WritePCLImage in length, at line 659 of ImageMagick@@ImageMagick6-6.9.10-85-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 659 of ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Line	956	956
Object	length	length

Code Snippet

File Name ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c

Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=29
Status	New

The size of the buffer used by WritePCLImage in pixels, at line 659 of ImageMagick@@ImageMagick6-6.9.10-85-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 659 of ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Line	957	957
Object	pixels	pixels

Code Snippet

File Name	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Method	static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=30
Status	New

The size of the buffer used by WritePCLImage in length, at line 659 of ImageMagick@@ImageMagick6-6.9.11-25-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 659 of ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Line	956	956
Object	length	length

Code Snippet

File Name	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Method	static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=31
Status	New

The size of the buffer used by WritePCLImage in pixels, at line 659 of ImageMagick@@ImageMagick6-6.9.11-25-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 659 of ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Line	957	957

Object	pixels	pixels

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=32
Status	New

The size of the buffer used by WritePCLImage in length, at line 659 of ImageMagick@@ImageMagick6-6.9.11-36-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 659 of ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Line	956	956
Object	length	length

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=33
Status	New

The size of the buffer used by WritePCLImage in pixels, at line 659 of ImageMagick@@ImageMagick6-6.9.11-36-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 659 of ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination

File	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Line	957	957
Object	pixels	pixels

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=34
Status	New

The size of the buffer used by WritePCLImage in length, at line 668 of ImageMagick@@ImageMagick6-6.9.11-62-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 668 of ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Line	965	965
Object	length	length

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=35
Status	New

The size of the buffer used by WritePCLImage in pixels, at line 668 of ImageMagick@@ImageMagick6-6.9.11-62-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 668 of ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Line	966	966
Object	pixels	pixels

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=36
Status New

The size of the buffer used by WritePCLImage in length, at line 659 of ImageMagick@@ImageMagick6-6.9.11-7-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 659 of ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Line	956	956
Object	length	length

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=37
Status New

The size of the buffer used by WritePCLImage in pixels, at line 659 of ImageMagick@@ImageMagick6-6.9.11-7-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 659 of ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Line	957	957
Object	pixels	pixels

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=38
Status New

The size of the buffer used by WritePCLImage in length, at line 668 of ImageMagick@@ImageMagick6-6.9.12-12-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 668 of ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c
Line	965	965
Object	length	length

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 21:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=39
Status	New

The size of the buffer used by WritePCLImage in pixels, at line 668 of ImageMagick@@ImageMagick6-6.9.12-12-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 668 of ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c
Line	966	966
Object	pixels	pixels

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=40
Status	New

The size of the buffer used by WritePCLImage in length, at line 668 of ImageMagick@@ImageMagick6-6.9.12-20-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 668 of ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c
Line	966	966
Object	length	length

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=41
Status	New

The size of the buffer used by WritePCLImage in pixels, at line 668 of ImageMagick@@ImageMagick6-6.9.12-20-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 668 of ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c
Line	967	967
Object	pixels	pixels

Code Snippet

File Name ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c

Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=42
Status	New

The size of the buffer used by WritePCLImage in length, at line 669 of ImageMagick@@ImageMagick6-6.9.12-32-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 669 of ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c
Line	967	967
Object	length	length

Code Snippet

File Name ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c

Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=43
Status	New

The size of the buffer used by WritePCLImage in pixels, at line 669 of ImageMagick@@ImageMagick6-6.9.12-32-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 669 of ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c
Line	968	968
Object	pixels	pixels

Code Snippet

File Name ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c

Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=44
Status	New

The size of the buffer used by WritePCLImage in length, at line 669 of ImageMagick@@ImageMagick6-6.9.12-42-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 669 of ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c
Line	967	967
Object	length	length

Code Snippet

File Name	ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c
Method	static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=45
Status	New

The size of the buffer used by WritePCLImage in pixels, at line 669 of ImageMagick@@ImageMagick6-6.9.12-42-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 669 of ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c
Line	968	968
Object	pixels	pixels

Code Snippet

File Name	ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c
Method	static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=46
Status	New

The size of the buffer used by *ReadDCMImage in clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-19-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 clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c

Line	3279	3279
Object	clone_info	clone_info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3279.            (void) memcpy(clone_info->scale,info.scale,clone_info->scale_size*
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=47
Status	New

The size of the buffer used by *ReadDCMImage in clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-19-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 clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	3280	3280
Object	clone_info	clone_info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3280.              sizeof(*clone_info->scale));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=48
Status	New

The size of the buffer used by *ReadDCMImage in clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-26-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

clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3279	3279
Object	clone_info	clone_info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3279.            (void) memcpy(clone_info->scale,info.scale,clone_info->scale_size*
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=49
Status New

The size of the buffer used by *ReadDCMImage in clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-26-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 clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3280	3280
Object	clone_info	clone_info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3280.              sizeof(*clone_info->scale));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20

	030&pathid=50
Status	New

The size of the buffer used by *ReadDCMImage in clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-30-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 clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3279	3279
Object	clone_info	clone_info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3279.            (void) memcpy(clone_info->scale,info.scale,clone_info->scale_size*
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=51
Status	New

The size of the buffer used by *ReadDCMImage in clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-30-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 clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3280	3280
Object	clone_info	clone_info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3280.              sizeof(*clone_info->scale));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=52
Status	New

The size of the buffer used by *ReadDCMImage in clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-35-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 clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3279	3279
Object	clone_info	clone_info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3279.            (void) memcpy(clone_info->scale,info.scale,clone_info->scale_size*
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=53
Status	New

The size of the buffer used by *ReadDCMImage in clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-35-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 clone_info, at line 3048 of ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3280	3280
Object	clone_info	clone_info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c

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

```
....
3280.              sizeof(*clone_info->scale));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=54
Status	New

The size of the buffer used by *ReadDCMImage in clone_info, at line 3052 of ImageMagick@@ImageMagick-7.1.1-4-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 clone_info, at line 3052 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	3285	3285
Object	clone_info	clone_info

Code Snippet

File Name	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3285.              (void) memcpy(clone_info->scale,info.scale,clone_info->scale_size*
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=55
Status	New

The size of the buffer used by *ReadDCMImage in clone_info, at line 3052 of ImageMagick@@ImageMagick-7.1.1-4-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 clone_info, at line 3052 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c

Line	3286	3286
Object	clone_info	clone_info

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3286.              sizeof(*clone_info->scale));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=56
Status	New

The size of the buffer used by deshufflePalette in image, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Line	215	215
Object	image	image

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
215.    (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=1020037&projectid=20030&pathid=57
Status	New

The size of the buffer used by deshufflePalette in oldColormap, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination

File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Line	216	216
Object	oldColormap	oldColormap

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=58
Status	New

The size of the buffer used by deshufflePalette in colors, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Line	223	223
Object	colors	colors

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
223.      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=1020037&projectid=20030&pathid=59
Status	New

The size of the buffer used by deshufflePalette in PixelInfo, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Line	224	224
Object	PixelInfo	PixelInfo

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
224.         sizeof(PixelInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=60
Status	New

The size of the buffer used by deshufflePalette in colors, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Line	225	225
Object	colors	colors

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
225.       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=1020037&projectid=20030&pathid=61
Status	New

The size of the buffer used by deshufflePalette in PixelInfo, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Line	226	226
Object	PixelInfo	PixelInfo

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
226.         sizeof(PixelInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=62
Status New

The size of the buffer used by deshufflePalette in image, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Line	215	215
Object	image	image

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=63
Status New

The size of the buffer used by deshufflePalette in oldColormap, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Line	216	216
Object	oldColormap	oldColormap

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=64
Status New

The size of the buffer used by deshufflePalette in colors, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Line	223	223
Object	colors	colors

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20

	030&pathid=65
Status	New

The size of the buffer used by deshufflePalette in PixelInfo, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Line	224	224
Object	PixelInfo	PixelInfo

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
224.         sizeof(PixelInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=66
Status	New

The size of the buffer used by deshufflePalette in colors, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Line	225	225
Object	colors	colors

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=67
Status	New

The size of the buffer used by deshufflePalette in PixelInfo, at line 202 of ImageMagick@@ImageMagick-7.1.1-4-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 202 of ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Line	226	226
Object	PixelInfo	PixelInfo

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

```
....
226.         sizeof(PixelInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=68
Status	New

The size of the buffer used by WritePCLImage in length, at line 659 of ImageMagick@@ImageMagick6-6.9.10-85-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 659 of ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c, to overwrite the target buffer.

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Line	806	806
Object	length	length

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

```
....
806.       (void) memset(pixels,0,(length+1)*sizeof(*pixels));
```

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=1020037&projectid=20030&pathid=225
Status	New

The dangerous function, memcpy, was found in use at line 659 in ImageMagick@@ImageMagick6-6.9.10-85-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@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Line	956	956
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

```
....
956.            (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=1020037&projectid=20030&pathid=226
Status	New

The dangerous function, memcpy, was found in use at line 659 in ImageMagick@@ImageMagick6-6.9.11-25-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@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Line	956	956

Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=227
Status	New

The dangerous function, memcpy, was found in use at line 659 in ImageMagick@@ImageMagick6-6.9.11-36-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@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Line	956	956
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=228
Status	New

The dangerous function, memcpy, was found in use at line 668 in ImageMagick@@ImageMagick6-6.9.11-62-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@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Line	965	965
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

```
....
965.            (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=1020037&projectid=20030&pathid=229
Status	New

The dangerous function, memcpy, was found in use at line 659 in ImageMagick@@ImageMagick6-6.9.11-7-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@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Line	956	956
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=230
Status	New

The dangerous function, memcpy, was found in use at line 668 in ImageMagick@@ImageMagick6-6.9.12-12-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@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c
Line	965	965
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=231
Status	New

The dangerous function, memcpy, was found in use at line 668 in ImageMagick@@ImageMagick6-6.9.12-20-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@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c
Line	966	966
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20

	030&pathid=232
Status	New

The dangerous function, memcpy, was found in use at line 669 in ImageMagick@@ImageMagick6-6.9.12-32-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@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c
Line	967	967
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=233
Status	New

The dangerous function, memcpy, was found in use at line 669 in ImageMagick@@ImageMagick6-6.9.12-42-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@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c
Line	967	967
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c
Method static MagickBooleanType WritePCLImage(const ImageInfo *image_info,Image *image)

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

Dangerous Functions\Path 10:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=234
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-19-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-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	3259	3259
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3259.            (void) memcpy(&info,info_copy,sizeof(info));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=235
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-19-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-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	3271	3271
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3271.            (void) memcpy(clone_info,&info,sizeof(info));
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=236
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-19-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-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	3279	3279
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3279.            (void) memcpy(clone_info->scale,info.scale,clone_info->scale_size*
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=237
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-26-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-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3259	3259
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3259.            (void) memcpy(&info,info_copy,sizeof(info));
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=238
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-26-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-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3271	3271
Object	memcpy	memcpy

Code Snippet

File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c

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

```
....
3271.            (void) memcpy(clone_info,&info,sizeof(info));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=239
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-26-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-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3279	3279
Object	memcpy	memcpy

Code Snippet

File Name	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3279.            (void) memcpy(clone_info->scale,info.scale,clone_info-
>scale_size*
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=240
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-30-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-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3259	3259
Object	memcpy	memcpy

Code Snippet

File Name	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method	static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3259.            (void) memcpy(&info,info_copy,sizeof(info));
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=241
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-30-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-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3271	3271

Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3271.            (void) memcpy(clone_info,&info,sizeof(info));
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=242
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-30-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-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3279	3279
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3279.            (void) memcpy(clone_info->scale,info.scale,clone_info->scale_size*
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=243
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-35-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-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3259	3259
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3259.            (void) memcpy(&info,info_copy,sizeof(info));
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=244
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-35-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-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3271	3271
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3271.            (void) memcpy(clone_info,&info,sizeof(info));
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=245
Status	New

The dangerous function, memcpy, was found in use at line 3048 in ImageMagick@@ImageMagick-7.1.1-35-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-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3279	3279
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3279.            (void) memcpy(clone_info->scale,info.scale,clone_info->scale_size*
```

Dangerous Functions\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=246
Status New

The dangerous function, memcpy, was found in use at line 3052 in ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	3265	3265
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3265.            (void) memcpy(&info,info_copy,sizeof(info));
```

Dangerous Functions\Path 23:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=247
Status	New

The dangerous function, memcpy, was found in use at line 3052 in ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	3277	3277
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3277.            (void) memcpy(clone_info,&info,sizeof(info));
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=248
Status	New

The dangerous function, memcpy, was found in use at line 3052 in ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	3285	3285
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3285.            (void) memcpy(clone_info->scale,info.scale,clone_info->scale_size*
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=249
Status	New

The dangerous function, memcpy, was found in use at line 202 in ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Line	215	215
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=250
Status	New

The dangerous function, memcpy, was found in use at line 202 in ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Line	223	223
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=251
Status	New

The dangerous function, memcpy, was found in use at line 202 in ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2023-34474-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Line	225	225
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34474-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=252
Status	New

The dangerous function, memcpy, was found in use at line 202 in ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Line	215	215
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=253
Status	New

The dangerous function, memcpy, was found in use at line 202 in ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Line	223	223
Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=254
Status	New

The dangerous function, memcpy, was found in use at line 202 in ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2023-34475-TP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Line	225	225

Object	memcpy	memcpy

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2023-34475-TP.c
Method static inline void deshufflePalette(Image *image,PixelInfo* oldColormap)

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

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=255
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.10-85-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@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Line	275	275
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.10-85-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 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=256
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.10-85-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@@ImageMagick6-6.9.10-	ImageMagick@@ImageMagick6-6.9.10-

	85-CVE-2022-32546-TP.c	85-CVE-2022-32546-TP.c
Line	278	278
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.10-85-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 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=257
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.10-85-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@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Line	286	286
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.10-85-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 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=258
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.10-85-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@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Line	289	289
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.10-85-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 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=259
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-25-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@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Line	275	275
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-25-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 36:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=260
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-25-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@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Line	278	278
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-25-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 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=261
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-25-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@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Line	286	286
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-25-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 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=262
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-25-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@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Line	289	289
Object	sscanf	sscanf

Code Snippet

File Name ImageMagick@@ImageMagick6-6.9.11-25-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 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=263
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-36-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@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Line	275	275
Object	sscanf	sscanf

Code Snippet

File Name ImageMagick@@ImageMagick6-6.9.11-36-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 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=264
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-36-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@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Line	278	278
Object	sscanf	sscanf

Code Snippet

File Name ImageMagick@@ImageMagick6-6.9.11-36-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 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=265
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-36-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@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Line	286	286
Object	sscanf	sscanf

Code Snippet	
File Name	ImageMagick@@ImageMagick6-6.9.11-36-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 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=266
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-36-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@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Line	289	289
Object	sscanf	sscanf

Code Snippet	
File Name	ImageMagick@@ImageMagick6-6.9.11-36-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 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=267
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-62-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@@ImageMagick6-6.9.11-	ImageMagick@@ImageMagick6-6.9.11-

	62-CVE-2022-32546-TP.c	62-CVE-2022-32546-TP.c
Line	275	275
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-62-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 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=268
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-62-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@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Line	278	278
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-62-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 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=269
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-62-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@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Line	286	286
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-62-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 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=270
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-62-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@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Line	289	289
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-62-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 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=271
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-7-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@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Line	275	275
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-7-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 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=272
Status New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-7-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@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Line	278	278
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-7-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 49:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=273
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-7-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@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Line	286	286
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-7-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 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=274
Status	New

The dangerous function, sscanf, was found in use at line 146 in ImageMagick@@ImageMagick6-6.9.11-7-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@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Line	289	289
Object	sscanf	sscanf

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-7-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",
```

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=1020037&projectid=20030&pathid=195
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2838 of ImageMagick@@ImageMagick-7.1.1-19-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-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	2922	2922
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2922.                index=(int) scaled_value;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=196
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2838 of ImageMagick@@ImageMagick-7.1.1-19-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-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	2939	2939
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2939.                          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=1020037&projectid=20030&pathid=197
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2838 of ImageMagick@@ImageMagick-7.1.1-26-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-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	2922	2922
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2922.                index=(int) scaled_value;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=198
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2838 of ImageMagick@@ImageMagick-7.1.1-26-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-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	2939	2939
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2939.                          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=1020037&projectid=20030&pathid=199
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2838 of ImageMagick@@ImageMagick-7.1.1-30-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-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	2922	2922
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2922.                index=(int) scaled_value;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=200
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2838 of ImageMagick@@ImageMagick-7.1.1-30-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-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	2939	2939
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2939.                          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=1020037&projectid=20030&pathid=201
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2838 of ImageMagick@@ImageMagick-7.1.1-35-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-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	2922	2922
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2922.                index=(int) scaled_value;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=202
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2838 of ImageMagick@@ImageMagick-7.1.1-35-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-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	2939	2939
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2939.                          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=1020037&projectid=20030&pathid=203
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2842 of ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	2926	2926
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2926.                index=(int) scaled_value;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=204
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2842 of ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	2943	2943
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static MagickBooleanType ReadDCMPixels(Image *image,DCMInfo *info,

```
....
2943.                          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=1020037&projectid=20030&pathid=205
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-19-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-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	3650	3650
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3650.                datum=(int) colors;
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=206
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-19-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-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	3677	3677
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3677.                datum=(int) colors;
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=207
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-19-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-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	3709	3709
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3709.                datum=(int) colors;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=208
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-19-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-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	3741	3741
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3741.                datum=(int) colors;
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=209
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-26-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-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3650	3650
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3650.                datum=(int) colors;
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=210
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-26-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-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3677	3677
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3677.                datum=(int) colors;
```

Integer Overflow\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=211
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-26-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-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3709	3709
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3709.                datum=(int) colors;
```

Integer Overflow\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=212

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-26-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-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3741	3741
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3741.                datum=(int) colors;
```

Integer Overflow\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=213
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-30-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-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3650	3650
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3650.                datum=(int) colors;
```

Integer Overflow\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20

	030&pathid=214
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-30-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-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3677	3677
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3677.                datum=(int) colors;
```

Integer Overflow\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=215
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-30-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-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3709	3709
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3709.                datum=(int) colors;
```

Integer Overflow\Path 22:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=216
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-30-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-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3741	3741
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3741.                datum=(int) colors;
```

Integer Overflow\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=217
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-35-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-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3650	3650
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3650.                datum=(int) colors;
```

Integer Overflow\Path 24:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=218
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-35-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-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3677	3677
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3677.                datum=(int) colors;
```

Integer Overflow\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=219
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-35-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-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3709	3709
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3709.                datum=(int) colors;
```

Integer Overflow\Path 26:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=220
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3048 of ImageMagick@@ImageMagick-7.1.1-35-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-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3741	3741
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3741.                datum=(int) colors;
```

Integer Overflow\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=221
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3052 of ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	3656	3656
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3656.                datum=(int) colors;
```

Integer Overflow\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=222
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3052 of ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	3683	3683
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3683.                datum=(int) colors;
```

Integer Overflow\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=223
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3052 of ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	3715	3715
Object	AssignExpr	AssignExpr

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3715.                datum=(int) colors;
```

Integer Overflow\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=224
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3052 of ImageMagick@@ImageMagick-7.1.1-4-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-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	3747	3747
Object	AssignExpr	AssignExpr

Code Snippet

File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c

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

```
....
3747.                datum=(int) colors;
```

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=1020037&projectid=20030&pathid=1
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c at line 258 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@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c
Line	279	279

Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c
Method static wchar_t *ConvertUTF8ToUTF16(const unsigned char *source)

```
....
279.        for (i=0; i <= (ssize_t) length; 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=1020037&projectid=20030&pathid=2
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c at line 558 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@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Line	648	648
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
648.          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=1020037&projectid=20030&pathid=3
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c at line 258 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@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c
Line	279	279

Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c
Method static wchar_t *ConvertUTF8ToUTF16(const unsigned char *source)

```
....
279.        for (i=0; i <= (ssize_t) length; 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=1020037&projectid=20030&pathid=4
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c at line 558 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@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Line	648	648
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
648.          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=1020037&projectid=20030&pathid=5
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c at line 258 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@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c
Line	279	279

Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c
Method static wchar_t *ConvertUTF8ToUTF16(const unsigned char *source)

```
....
279.        for (i=0; i <= (ssize_t) length; 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=1020037&projectid=20030&pathid=6
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c at line 558 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@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Line	648	648
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
648.          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=1020037&projectid=20030&pathid=7
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c at line 567 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@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Line	657	657

Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-62-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
657.          for (j=0; j <= (ssize_t) count; j++)
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=8
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c at line 258 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@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c
Line	279	279
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c
Method static wchar_t *ConvertUTF8ToUTF16(const unsigned char *source)

```
....
279.        for (i=0; i <= (ssize_t) length; i++)
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=9
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c at line 558 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@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Line	648	648

Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
648.          for (j=0; j <= (ssize_t) count; j++)
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=10
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c at line 567 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@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c
Line	657	657
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-12-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
657.          for (j=0; j <= (ssize_t) count; j++)
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=11
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c at line 567 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@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c
Line	657	657

Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-20-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
657.          for (j=0; j <= (ssize_t) count; j++)
```

Potential Off by One Error in Loops\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=12
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c at line 568 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@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c
Line	658	658
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-32-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
658.          for (j=0; j <= (ssize_t) count; j++)
```

Potential Off by One Error in Loops\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=13
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c at line 568 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@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c	ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c
Line	658	658

Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.12-42-CVE-2022-32546-TP.c
Method static size_t PCLPackbitsCompressImage(const size_t length,

```
....
658.          for (j=0; j <= (ssize_t) count; j++)
```

Potential Off by One Error in Loops\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=14
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c at line 3048 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-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	4032	4032
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
4032.          for (i=0; i <= (ssize_t) GetQuantumRange(info.depth);
i++)
```

Potential Off by One Error in Loops\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=15
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c at line 3048 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-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c

Line	4032	4032
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
4032.          for (i=0; i <= (ssize_t) GetQuantumRange(info.depth);
i++)
```

Potential Off by One Error in Loops\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=16
Status New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c at line 3048 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-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	4032	4032
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
4032.          for (i=0; i <= (ssize_t) GetQuantumRange(info.depth);
i++)
```

Potential Off by One Error in Loops\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=17
Status New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c at line 3048 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-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	4032	4032
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
4032.          for (i=0; i <= (ssize_t) GetQuantumRange(info.depth);
i++)
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=18
Status	New

The buffer allocated by <= in ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c at line 3052 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-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	4038	4038
Object	<=	<=

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
4038.          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=1020037&projectid=20030&pathid=332
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c
Line	3974	3974
Object	fputc	fputc

Code Snippet

File Name ImageMagick@@ImageMagick-7.1.1-19-CVE-2021-3962-FP.c

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

```
....
3974.               if (fputc(c,file) != c)
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=333
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c
Line	3974	3974
Object	fputc	fputc

Code Snippet

File Name ImageMagick@@ImageMagick-7.1.1-26-CVE-2021-3962-FP.c

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

```
....
3974.               if (fputc(c,file) != c)
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20

	030&pathid=334
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Line	3974	3974
Object	fputc	fputc

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-30-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3974.               if (fputc(c,file) != c)
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=335
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Line	3974	3974
Object	fputc	fputc

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-35-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3974.               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=1020037&projectid=20030&pathid=336
Status	New

	Source	Destination

File	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c	ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Line	3980	3980
Object	fputc	fputc

Code Snippet
File Name ImageMagick@@ImageMagick-7.1.1-4-CVE-2021-3962-FP.c
Method static Image *ReadDCMImage(const ImageInfo *image_info,ExceptionInfo *exception)

```
....
3980.              if (fputc(c,file) != c)
```

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=1020037&projectid=20030&pathid=337
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c
Line	401	401
Object	CreateFile	CreateFile

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.10-85-CVE-2022-32545-TP.c
Method static HENHMETAFILE ReadEnhMetaFile(const char *path,ssize_t *width,

```
....
401.
hFile=CreateFile(path,GENERIC_READ,0,NULL,OPEN_EXISTING,FILE_ATTRIBUTE_NORMAL,
```

Incorrect Permission Assignment For Critical Resources\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=338
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c
Line	401	401
Object	CreateFile	CreateFile

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-25-CVE-2022-32545-TP.c
Method static HENHMETAFILE ReadEnhMetaFile(const char *path,ssize_t *width,

```
....
401.
hFile=CreateFile(path,GENERIC_READ,0,NULL,OPEN_EXISTING,FILE_ATTRIBUTE_N
ORMAL,
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=339
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c
Line	401	401
Object	CreateFile	CreateFile

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-36-CVE-2022-32545-TP.c
Method static HENHMETAFILE ReadEnhMetaFile(const char *path,ssize_t *width,

```
....
401.
hFile=CreateFile(path,GENERIC_READ,0,NULL,OPEN_EXISTING,FILE_ATTRIBUTE_N
ORMAL,
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020037&projectid=20030&pathid=340
Status	New

	Source	Destination
File	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c	ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c
Line	401	401
Object	CreateFile	CreateFile

Code Snippet
File Name ImageMagick@@ImageMagick6-6.9.11-7-CVE-2022-32545-TP.c
Method static HENHMETAFILE ReadEnhMetaFile(const char *path,ssize_t *width,

```
....
401.
hFile=CreateFile(path,GENERIC_READ,0,NULL,OPEN_EXISTING,FILE_ATTRIBUTE_N
ORMAL,
```

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));
    }
}
```

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;
}
```

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

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025