vul_files_39 Scan Report

Project Name	vul_files_39
Scan Start	Wednesday, January 8, 2025 10:51:33 AM
Preset	Checkmarx Default
Scan Time	03h:23m:18s
Lines Of Code Scanned	299665
Files Scanned	141
Report Creation Time	Wednesday, January 8, 2025 2:23:57 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	1/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

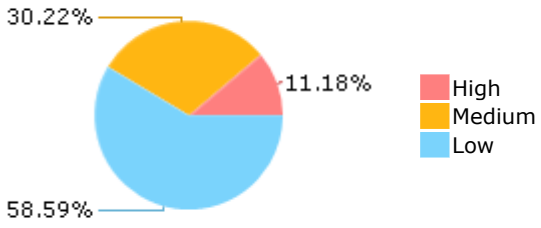
Results Limit

Results limit per query was set to 50

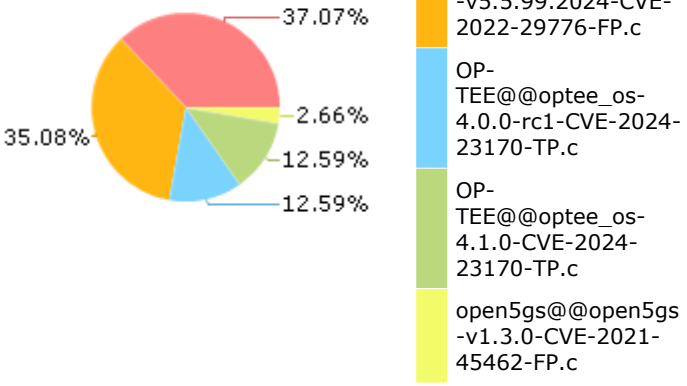
Selected Queries

Selected queries are listed in Result Summary

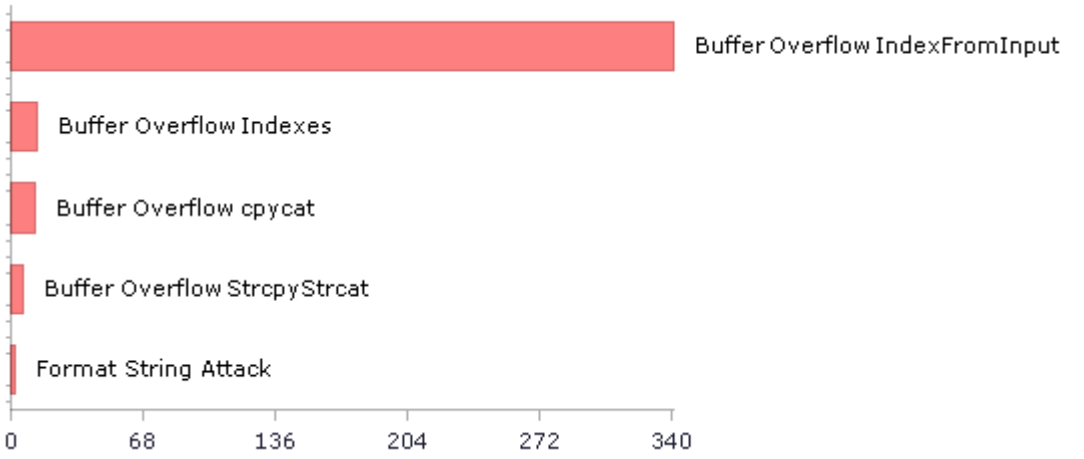
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	1433	391
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	482	482
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	4	4
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	534	534
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	534	534
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	44	44
PCI DSS (3.2) - 6.5.2 - Buffer overflows	324	205
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.	55	55
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.	74	74
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.	8	8
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.	427	427
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.	2	2
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	36	36

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

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	490	490
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)	2	2
SC-4 Information in Shared Resources (P1)	2	2
SC-5 Denial of Service Protection (P1)*	851	245
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	484	409
SI-11 Error Handling (P2)*	97	97
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	166	76

***** 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

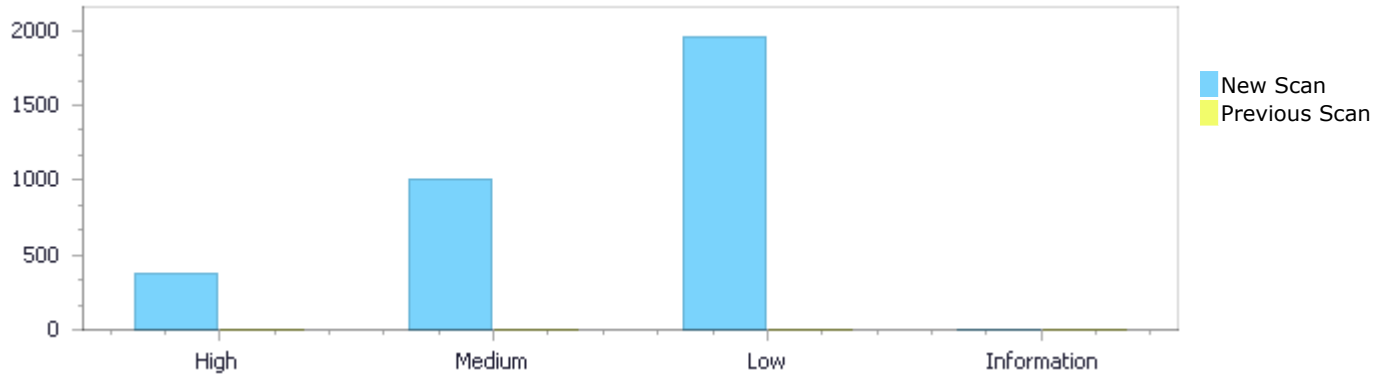
	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, 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	374	1,011	1,960	0	3,345
Recurrent Issues	0	0	0	0	0
Total	374	1,011	1,960	0	3,345
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	374	1,011	1,960	0	3,345
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	374	1,011	1,960	0	3,345

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	341	High
Buffer Overflow Indexes	13	High
Buffer Overflow cpycat	12	High
Buffer Overflow StrcpyStrcat	6	High
Format String Attack	2	High

Dangerous Functions	534	Medium
Buffer Overflow boundcpy WrongSizeParam	121	Medium
Buffer Overflow Loops	118	Medium
Stored Buffer Overflow boundcpy	47	Medium
Use of Zero Initialized Pointer	37	Medium
Uncontrolled Recursion	34	Medium
Divide By Zero	26	Medium
Use of Uninitialized Pointer	24	Medium
Integer Overflow	14	Medium
Float Overflow	12	Medium
Short Overflow	10	Medium
MemoryFree on StackVariable	7	Medium
Stored Buffer Overflow cpycat	6	Medium
Memory Leak	5	Medium
Buffer Overflow AddressOfLocalVarReturned	4	Medium
Use of Uninitialized Variable	4	Medium
Char Overflow	2	Medium
Double Free	2	Medium
Off by One Error in Loops	2	Medium
Wrong Size t Allocation	2	Medium
NULL Pointer Dereference	703	Low
Improper Resource Access Authorization	427	Low
Unchecked Array Index	346	Low
Use of Sizeof On a Pointer Type	128	Low
Unchecked Return Value	97	Low
Arithmenic Operation On Boolean	74	Low
TOCTOU	58	Low
Incorrect Permission Assignment For Critical Resources	55	Low
Potential Off by One Error in Loops	44	Low
Exposure of System Data to Unauthorized Control Sphere	8	Low
Heuristic 2nd Order Buffer Overflow malloc	8	Low
Potential Precision Problem	6	Low
Insecure Temporary File	2	Low
Sizeof Pointer Argument	2	Low
Use of Insufficiently Random Values	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	513
ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	468
open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	26
OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	19
OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c	19
open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c	14
open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c	14
open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c	14
ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c	8
open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c	7

Scan Results Details

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=34
Status	New

The size of the buffer used by main in argc, at line 8313 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argc, at line 8313 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8313	8381
Object	argc	argc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8313.  int CLASS main (int argc, char **argv)
....
8381.    argv[argc] = "";
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=35
Status	New

The size of the buffer used by main in argc, at line 8313 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argc, at line 8313 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination

File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8313	8381
Object	argc	argc

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8313.  int CLASS main (int argc, char **argv)
....
8381.    argv[argc] = "";
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=36
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4831	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.        fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=37
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4842	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.       fscanf (ifp, "%f", &romm_cam[0][i]);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 5:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=38
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4846	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4846.        fscanf (ifp, "%d", &planes);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 6:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=39
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4848	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4848.         fscanf (ifp, "%d", &flip);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=40
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4851	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.       fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=41
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4855	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.        fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=42
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=43
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.        fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=44
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-	ONLYOFFICE@@core-v5.5.99.2024-CVE-

	2022-29776-FP.c	2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=45
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4831	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=46
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable

a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4842	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.       fscanf (ifp, "%f", &romm_cam[0][i]);
....
4867.       (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 14:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=47
Status New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4846	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4846.        fscanf (ifp, "%d", &planes);
....
4867.       (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 15:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=48
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4848	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4848.         fscanf (ifp, "%d", &flip);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=49
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4848	4867
Object	Address	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4848.         fscanf (ifp, "%d", &flip);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=50
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4831	4802
Object	ifp	i

Code Snippet

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Method void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.       cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=51
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4842	4802
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.       fscanf (ifp, "%f", &romm_cam[0][i]);
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Method void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.       cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=52
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4842	4802
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.       fscanf (ifp, "%f", &romm_cam[0][i]);
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Method void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.       cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=53
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4831	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=54
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4842	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.       fscanf (ifp, "%f", &romm_cam[0][i]);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=55
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4846	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4846.        fscanf (ifp, "%d", &planes);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=56
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4848	4833
Object	ifp	i

Code Snippet	
File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS parse_mos (int offset)

```
....
4848.         fscanf (ifp, "%d", &flip);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=57
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4851	4833
Object	ifp	i

Code Snippet	
File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS parse_mos (int offset)

```
....
4851.        fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=58
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-	ONLYOFFICE@@core-v99.99.99.2148-

	CVE-2022-29776-FP.c	CVE-2022-29776-FP.c
Line	4855	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=59
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4859	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4859.         FORC4 fscanf (ifp, "%d", neut+c);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=60
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 28:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=61
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.        fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 29:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=62
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow IndexFromInput\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=63
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4831	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=64
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4842	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.       fscanf (ifp, "%f", &romm_cam[0][i]);
....
4867.       (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=65
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4846	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4846.         fscanf (ifp, "%d", &planes);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=66
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4848	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4848.         fscanf (ifp, "%d", &flip);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=67
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4851	4867
Object	ifp	BinaryExpr

Code Snippet	
File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS parse_mos (int offset)

```
....
4851.       fscanf (ifp, "%d", &i);
....
4867.       (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=68
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4855	4867
Object	ifp	BinaryExpr

Code Snippet	
File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS parse_mos (int offset)

```
....
4855.        fscanf (ifp, "%d", &i);
....
4867.       (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=69
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-	ONLYOFFICE@@core-v99.99.99.2148-

	CVE-2022-29776-FP.c	CVE-2022-29776-FP.c
Line	4859	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4859.         FORC4 fscanf (ifp, "%d", neut+c);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=70
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4848	4867
Object	Address	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4848.         fscanf (ifp, "%d", &flip);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow IndexFromInput\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=71
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4831	4802
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.       cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 39:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=72
Status New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4842	4802
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.       fscanf (ifp, "%f", &romm_cam[0][i]);
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.        cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=73
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4846	4802
Object	ifp	i

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS parse_mos (int offset)

```
....
4846.        fscanf (ifp, "%d", &planes);
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.        cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=74
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4848	4802
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4848.         fscanf (ifp, "%d", &flip);
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.       cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 42:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=75
Status New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getreal passes to fgetc, at line 318 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	338	4802
Object	fgetc	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method double CLASS getreal (int type)

```
....
338.      default: return fgetc(ifp);
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.        cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=76
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get2 passes to str, at line 283 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	286	4802
Object	str	i

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	ushort CLASS get2()

```
....
286.    fread (str, 1, 2, ifp);
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.        cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=77
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that get4 passes to str, at line 299 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	302	4802
Object	str	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method unsigned CLASS get4()

```
....
302.    fread (str, 1, 4, ifp);
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.       cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 45:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=78
Status New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4842	4802
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.       fscanf (ifp, "%f", &romm_cam[0][i]);
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS romm_coeff (float romm_cam[3][3])

```
....
4802.        cmatrix[i][j] += rgb_romm[i][k] * romm_cam[k][j];
```

Buffer Overflow IndexFromInput\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=79
Status	New

The size of the buffer used by phase_one_correct in i, at line 1479 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getreal passes to fgetc, at line 318 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	338	1579
Object	fgetc	i

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	double CLASS getreal (int type)

```
....
338.      default: return fgetc(ifp);
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS phase_one_correct()

```
....
1579.        yval[i][j] = getreal(11);
```

Buffer Overflow IndexFromInput\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=80
Status	New

The size of the buffer used by phase_one_correct in i, at line 1479 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that get2 passes to str, at line 283 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	286	1579
Object	str	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method ushort CLASS get2()

```
....
286.    fread (str, 1, 2, ifp);
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS phase_one_correct()

```
....
1579.       yval[i][j] = getreal(11);
```

Buffer Overflow IndexFromInput\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=81
Status	New

The size of the buffer used by phase_one_correct in i, at line 1479 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get4 passes to str, at line 299 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	302	1579
Object	str	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS get4()

```
....
302.    fread (str, 1, 4, ifp);
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS phase_one_correct()

```
....
1579.       yval[i][j] = getreal(11);
```

Buffer Overflow IndexFromInput\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=82
Status	New

The size of the buffer used by lossless_jpeg_load_raw in BinaryExpr, at line 927 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	943
Object	fgetc	BinaryExpr

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS lossless_jpeg_load_raw()

```
....
943.        val = curve[val & 0xfff];
```

Buffer Overflow IndexFromInput\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=83
Status	New

The size of the buffer used by canon_sraw_load_raw in BinaryExpr, at line 972 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable

a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	994
Object	fgetc	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS canon_sraw_load_raw()

```
....
994.          ip[col + (c >> 1)*width + (c & 1)][0] = rp[jcol+c];
```

Buffer Overflow Indexes

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

Categories

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

Description
Buffer Overflow Indexes\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=7
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4831	4867
Object	ifp	flip

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=8
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4842	4867
Object	ifp	flip

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS parse_mos (int offset)

```
....
4842.        fscanf (ifp, "%f", &romm_cam[0][i]);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=9
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-	ONLYOFFICE@@core-v5.5.99.2024-CVE-

	2022-29776-FP.c	2022-29776-FP.c
Line	4846	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4846.         fscanf (ifp, "%d", &planes);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=10
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4848	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4848.         fscanf (ifp, "%d", &flip);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=11
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4851	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.       fscanf (ifp, "%d", &i);
....
4867.       (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=12
Status New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4855	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.        fscanf (ifp, "%d", &i);
....
4867.       (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 7:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=13
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4831	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=14
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4842	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.        fscanf (ifp, "%f", &romm_cam[0][i]);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=15
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4846	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4846.         fscanf (ifp, "%d", &planes);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=16
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4848	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4848.         fscanf (ifp, "%d", &flip);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=17
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4851	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.        fscanf (ifp, "%d", &i);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=18
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4855	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.         fscanf (ifp, "%d", &i);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow Indexes\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=19
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to ifp, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4859	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4859.         FORC4 fscanf (ifp, "%d", neut+c);
....
4867.        (uchar) "\x94\x61\x16\x49"[(flip/90 + frot) & 3];
```

Buffer Overflow cpycat

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

Categories

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

Description

Buffer Overflow cpycat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=1
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.        fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Method void CLASS parse_mos (int offset)

```
....
4855.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=4
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=5
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.       fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=6
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=20
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=21
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-	ONLYOFFICE@@core-v5.5.99.2024-CVE-

	2022-29776-FP.c	2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.       fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=22
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.        fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=23
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 11:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=24
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.        fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow cpycat\Path 12:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=25
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow StrcpyStrcat

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

Categories

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

Description
Buffer Overflow StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=28
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=29
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.        fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=30
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=31
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=32
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.       fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=33
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.        fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Format String Attack

Query Path:
CPP\Cx\CPP Buffer Overflow\Format String Attack Version:1

Categories

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

OWASP Top 10 2017: A1-Injection

Description

Format String Attack\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=26
Status	New

Method parse_riff at line 5849 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c receives the "%*s %s %d %d:%d:%d %d" value from user input. This value is then used to construct a "format string" "%*s %s %d %d:%d:%d %d", which is provided as an argument to a string formatting function in parse_riff method of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 5849.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5877	5877
Object	"%*s %s %d %d:%d:%d %d"	"%*s %s %d %d:%d:%d %d"

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_riff()

```
....
5877.      if (sscanf (date, "%*s %s %d %d:%d:%d %d", month, &t.tm_mday,
```

Format String Attack\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=27
Status	New

Method parse_riff at line 5849 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c receives the "%*s %s %d %d:%d:%d %d" value from user input. This value is then used to construct a "format string" "%*s %s %d %d:%d:%d %d", which is provided as an argument to a string formatting function in parse_riff method of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 5849.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5877	5877
Object	"%*s %s %d %d:%d:%d %d"	"%*s %s %d %d:%d:%d %d"

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_riff()

```
....
5877.      if (sscanf (date, "%*s %s %d %d:%d:%d %d", month, &t.tm_mday,
```

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=1020062&projectid=20045&pathid=660
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.0.22-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	open5gs@@open5gs-v2.0.22-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.0.22-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.0.22-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=661
Status	New

The dangerous function, _alloca, was found in use at line 53 in open5gs@@open5gs-v2.2.0-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	open5gs@@open5gs-v2.2.0-CVE-2023-46752-FP.c	open5gs@@open5gs-v2.2.0-CVE-2023-46752-FP.c
Line	191	191
Object	_alloca	_alloca

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2023-46752-FP.c
Method int ogs_proc_create(const char *const commandLine[], int options,

```
....
191.      commandLineCombined = (char *)_alloca(len);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=662
Status	New

The dangerous function, _snprintf, was found in use at line 8313 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8655	8655
Object	_snprintf	_snprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8655.             snprintf(0,0,"%d",is_raw-1), shot_select);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=663
Status	New

The dangerous function, _snprintf, was found in use at line 8313 in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8655	8655
Object	_snprintf	_snprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8655.             snprintf(0,0,"%d",is_raw-1), shot_select);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=664
Status	New

The dangerous function, memcpy, was found in use at line 932 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1014	1014
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantizePixels(PIX *pixs,

```
....
1014.              memcpy(buf1r, buf2r, 4 * w);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=665
Status	New

The dangerous function, memcpy, was found in use at line 932 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1015	1015
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantizePixels(PIX *pixs,

```
....
1015.              memcpy(buf1g, buf2g, 4 * w);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=666
Status	New

The dangerous function, memcpy, was found in use at line 932 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1016	1016
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantizePixels(PIX *pixs,

```
....
1016.              memcpy(buf1b, buf2b, 4 * w);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=667
Status	New

The dangerous function, memcpy, was found in use at line 1933 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1989	1989
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixDitherOctindexWithCmap(PIX *pixs,

```
....
1989.           memcpy(buf1r, buf2r, 4 * w);
```

Dangerous Functions\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=668
Status New

The dangerous function, memcpy, was found in use at line 1933 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1990	1990
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixDitherOctindexWithCmap(PIX *pixs,

```
....
1990.           memcpy(buf1g, buf2g, 4 * w);
```

Dangerous Functions\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=669
Status New

The dangerous function, memcpy, was found in use at line 1933 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1991	1991
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixDitherOctindexWithCmap(PIX *pixs,

```
....
1991.          memcpy(buf1b, buf2b, 4 * w);
```

Dangerous Functions\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=670
Status New

The dangerous function, memcpy, was found in use at line 8313 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8588	8588
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8588.        memcpy (rgb_cam, cmatrix, sizeof cmatrix);
```

Dangerous Functions\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=671
Status New

The dangerous function, memcpy, was found in use at line 2166 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2214	2214
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=672
Status	New

The dangerous function, memcpy, was found in use at line 2950 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2957	2957
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS foveon_fixed (void *ptr, int size, const char *name)

```
....
2957.    memcpy (ptr, dp, size*4);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=673
Status	New

The dangerous function, memcpy, was found in use at line 3014 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3116	3116
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3116.    memcpy (black, black+8, sizeof *black*8);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=674
Status	New

The dangerous function, memcpy, was found in use at line 3014 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3117	3117
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3117.    memcpy (black+height-11, black+height-22, 11*sizeof *black);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=675
Status	New

The dangerous function, memcpy, was found in use at line 3014 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3118	3118
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3118.    memcpy (last, black, sizeof last);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=676
Status	New

The dangerous function, memcpy, was found in use at line 3014 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3128	3128
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3128.      memcpy (last[2], black[row+1], sizeof last[2]);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=677
Status	New

The dangerous function, memcpy, was found in use at line 3014 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3134	3134
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3134.    memcpy (fsum, black, sizeof fsum);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=678
Status	New

The dangerous function, memcpy, was found in use at line 3014 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3138	3138
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3138.    memcpy (last[0], black[height-1], sizeof last[0]);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=679
Status	New

The dangerous function, memcpy, was found in use at line 3014 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3158	3158
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3158.       memcpy (prev, pix, sizeof prev);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=680
Status	New

The dangerous function, memcpy, was found in use at line 3014 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3368	3368
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3368.         memcpy (smrow[2], smrow[1], sizeof **smrow * width);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=681
Status	New

The dangerous function, memcpy, was found in use at line 3748 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3757	3757
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS scale_colors()

```
....
3757.      memcpy (pre_mul, user_mul, sizeof pre_mul);
```

Dangerous Functions\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=682
Status New

The dangerous function, memcpy, was found in use at line 3748 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3796	3796
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS scale_colors()

```
....
3796.        memcpy (pre_mul, cam_mul, sizeof pre_mul);
```

Dangerous Functions\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=683
Status New

The dangerous function, memcpy, was found in use at line 3962 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4054	4054
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4054.       memcpy (brow[2][col], pix, sizeof *image);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=684
Status	New

The dangerous function, memcpy, was found in use at line 3962 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4078	4078
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4078.       memcpy (image[(row-2)*width+2], brow[0]+2, (width-4)*sizeof
*image);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=685
Status	New

The dangerous function, memcpy, was found in use at line 3962 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4082	4082
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4082.    memcpy (image[(row-2)*width+2], brow[0]+2, (width-4)*sizeof
*image);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=686
Status	New

The dangerous function, memcpy, was found in use at line 3962 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4083	4083
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4083.    memcpy (image[(row-1)*width+2], brow[1]+2, (width-4)*sizeof
*image);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=687
Status	New

The dangerous function, memcpy, was found in use at line 4913 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5086	5086
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5086.       if (cfa == 070) memcpy (cfa_pc,"\003\004\005",3);     /* CMY
*/
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=688
Status	New

The dangerous function, memcpy, was found in use at line 4913 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5087	5087
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5087.       if (cfa == 072) memcpy (cfa_pc,"\005\003\004\001",4); /*
GMCY */
```

Dangerous Functions\Path 30:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=689
Status	New

The dangerous function, memcpy, was found in use at line 5481 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5500	5500
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_external_jpeg()

```
....
5500.         memcpy (jfile, file+4, 4);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=690
Status	New

The dangerous function, memcpy, was found in use at line 5481 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5501	5501
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_external_jpeg()

```
....
5501.         memcpy (jfile+4, file, 4);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=691
Status	New

The dangerous function, memcpy, was found in use at line 7910 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7967	7967
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7967.    memcpy (out_cam, rgb_cam, sizeof out_cam);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=692
Status	New

The dangerous function, memcpy, was found in use at line 7910 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7973	7973
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7973.      memcpy (oprof, phead, sizeof phead);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=693
Status	New

The dangerous function, memcpy, was found in use at line 7910 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7981	7981
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7981.       memcpy (oprof+32, pbody, sizeof pbody);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=694
Status	New

The dangerous function, memcpy, was found in use at line 7910 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7983	7983
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7983.       memcpy ((char *)oprof+pbody[8]+8, pwhite, sizeof pwhite);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=695
Status	New

The dangerous function, memcpy, was found in use at line 7910 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7987	7987
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7987.         memcpy ((char *)oprof+pbody[i*3+2], pcurve, sizeof pcurve);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=696
Status	New

The dangerous function, memcpy, was found in use at line 8175 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8231	8231
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS tiff_head (struct tiff_hdr *th, int full)

```
....
8231.       memcpy (th->gps, gpsdata, sizeof th->gps);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=697
Status	New

The dangerous function, memcpy, was found in use at line 8249 in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8261	8261
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS jpeg_thumb (FILE *tfp)

```
....
8261.       memcpy (exif, "\xff\xe1  Exif\0\0", 10);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=698
Status	New

The dangerous function, memcpy, was found in use at line 932 in ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1014	1014
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c

Method	pixOctreeQuantizePixels(PIX *pixs,

```
....
1014.              memcpy(buf1r, buf2r, 4 * w);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=699
Status	New

The dangerous function, memcpy, was found in use at line 932 in ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1015	1015
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantizePixels(PIX *pixs,

```
....
1015.              memcpy(buf1g, buf2g, 4 * w);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=700
Status	New

The dangerous function, memcpy, was found in use at line 932 in ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1016	1016
Object	memcpy	memcpy

Code Snippet

File Name	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method	pixOctreeQuantizePixels(PIX *pixs,

```
....
1016.              memcpy(buf1b, buf2b, 4 * w);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=701
Status	New

The dangerous function, memcpy, was found in use at line 1933 in ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1989	1989
Object	memcpy	memcpy

Code Snippet

File Name	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method	pixDitherOctindexWithCmap(PIX *pixs,

```
....
1989.          memcpy(buf1r, buf2r, 4 * w);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=702
Status	New

The dangerous function, memcpy, was found in use at line 1933 in ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1990	1990
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixDitherOctindexWithCmap(PIX *pixs,

```
....
1990.          memcpy(buf1g, buf2g, 4 * w);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=703
Status	New

The dangerous function, memcpy, was found in use at line 1933 in ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1991	1991
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixDitherOctindexWithCmap(PIX *pixs,

```
....
1991.          memcpy(buf1b, buf2b, 4 * w);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=704
Status	New

The dangerous function, memcpy, was found in use at line 932 in ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1014	1014
Object	memcpy	memcpy

Code Snippet	
File Name	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method	pixOctreeQuantizePixels(PIX *pixs,

```
....
1014.              memcpy(buf1r, buf2r, 4 * w);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=705
Status	New

The dangerous function, memcpy, was found in use at line 932 in ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1015	1015
Object	memcpy	memcpy

Code Snippet	
File Name	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method	pixOctreeQuantizePixels(PIX *pixs,

```
....
1015.              memcpy(buf1g, buf2g, 4 * w);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=706
Status	New

The dangerous function, memcpy, was found in use at line 932 in ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1016	1016

Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method pixOctreeQuantizePixels(PIX *pixs,

```
....
1016.              memcpy(buf1b, buf2b, 4 * w);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=707
Status	New

The dangerous function, memcpy, was found in use at line 1933 in ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1989	1989
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method pixDitherOctindexWithCmap(PIX *pixs,

```
....
1989.          memcpy(buf1r, buf2r, 4 * w);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=708
Status	New

The dangerous function, memcpy, was found in use at line 1933 in ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c

Line	1990	1990
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method pixDitherOctindexWithCmap(PIX *pixs,

```
....
1990.          memcpy(buf1g, buf2g, 4 * w);
```

Dangerous Functions\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=709
Status New

The dangerous function, memcpy, was found in use at line 1933 in ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1991	1991
Object	memcpy	memcpy

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method pixDitherOctindexWithCmap(PIX *pixs,

```
....
1991.          memcpy(buf1b, buf2b, 4 * w);
```

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=1020062&projectid=20045&pathid=379

Status	New

The size of the buffer used by main in cmatrix, at line 8313 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to cmatrix, at line 8313 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8588	8588
Object	cmatrix	cmatrix

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8588.         memcpy (rgb_cam, cmatrix, sizeof cmatrix);
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=380
Status	New

The size of the buffer used by foveon_interpolate in last, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that foveon_interpolate passes to last, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3128	3128
Object	last	last

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3128.       memcpy (last[2], black[row+1], sizeof last[2]);
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=381
Status	New

The size of the buffer used by foveon_interpolate in last, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that foveon_interpolate passes to last, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3138	3138
Object	last	last

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3138.    memcpy (last[0], black[height-1], sizeof last[0]);
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=382
Status	New

The size of the buffer used by vng_interpolate in image, at line 3962 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that vng_interpolate passes to image, at line 3962 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4054	4054
Object	image	image

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4054.        memcpy (brow[2][col], pix, sizeof *image);
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=383
Status	New

The size of the buffer used by convert_to_rgb in phead, at line 7910 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that convert_to_rgb passes to phead, at line 7910 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7973	7973
Object	phead	phead

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7973.       memcpy (oprof, phead, sizeof phead);
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=384
Status	New

The size of the buffer used by convert_to_rgb in pbody, at line 7910 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that convert_to_rgb passes to pbody, at line 7910 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7981	7981
Object	pbody	pbody

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7981.       memcpy (oprof+32, pbody, sizeof pbody);
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=385
Status	New

The size of the buffer used by convert_to_rgb in pwhite, at line 7910 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that convert_to_rgb passes to pwhite, at line 7910 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7983	7983
Object	pwhite	pwhite

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7983.      memcpy ((char *)oprof+pbody[8]+8, pwhite, sizeof pwhite);
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=386
Status	New

The size of the buffer used by convert_to_rgb in pcurve, at line 7910 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that convert_to_rgb passes to pcurve, at line 7910 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7987	7987
Object	pcurve	pcurve

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7987.        memcpy ((char *)oprof+pbody[i*3+2], pcurve, sizeof pcurve);
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=387
Status	New

The size of the buffer used by tiff_head in th, at line 8175 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tiff_head passes to th, at line 8175 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8231	8231
Object	th	th

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS tiff_head (struct tiff_hdr *th, int full)

```
....
8231.      memcpy (th->gps, gpsdata, sizeof th->gps);
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=388
Status	New

The size of the buffer used by main in cmatrix, at line 8313 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to cmatrix, at line 8313 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8588	8588
Object	cmatrix	cmatrix

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8588.        memcpy (rgb_cam, cmatrix, sizeof cmatrix);
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=389
Status	New

The size of the buffer used by foveon_interpolate in last, at line 3014 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that foveon_interpolate passes to last, at line 3014 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3128	3128
Object	last	last

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3128.      memcpy (last[2], black[row+1], sizeof last[2]);
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=390
Status	New

The size of the buffer used by foveon_interpolate in last, at line 3014 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that foveon_interpolate passes to last, at line 3014 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3138	3138
Object	last	last

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3138.    memcpy (last[0], black[height-1], sizeof last[0]);
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=391
Status	New

The size of the buffer used by vng_interpolate in image, at line 3962 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that vng_interpolate passes to image, at line 3962 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4054	4054
Object	image	image

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4054.       memcpy (brow[2][col], pix, sizeof *image);
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=392
Status	New

The size of the buffer used by convert_to_rgb in phead, at line 7910 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that convert_to_rgb passes to phead, at line 7910 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7973	7973
Object	phead	phead

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7973.      memcpy (oprof, phead, sizeof phead);
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=393
Status	New

The size of the buffer used by convert_to_rgb in pbody, at line 7910 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that convert_to_rgb passes to pbody, at line 7910 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7981	7981
Object	pbody	pbody

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7981.      memcpy (oprof+32, pbody, sizeof pbody);
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=394
Status	New

The size of the buffer used by convert_to_rgb in pwhite, at line 7910 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that convert_to_rgb passes to pwhite, at line 7910 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7983	7983
Object	pwhite	pwhite

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7983.       memcpy ((char *)oprof+pbody[8]+8, pwhite, sizeof pwhite);
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=395
Status	New

The size of the buffer used by convert_to_rgb in pcurve, at line 7910 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that convert_to_rgb passes to pcurve, at line 7910 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7987	7987
Object	pcurve	pcurve

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
7987.       memcpy ((char *)oprof+pbody[i*3+2], pcurve, sizeof pcurve);
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=396
Status	New

The size of the buffer used by tiff_head in th, at line 8175 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tiff_head passes to th, at line 8175 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8231	8231
Object	th	th

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method	void CLASS tiff_head (struct tiff_hdr *th, int full)

```
....
8231.      memcpy (th->gps, gpsdata, sizeof th->gps);
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=397
Status	New

The size of the buffer used by ogs_sock_bind in ->, at line 97 of open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ogs_sock_bind passes to ->, at line 97 of open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c
Line	115	115
Object	->	->

Code Snippet	
File Name	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c
Method	int ogs_sock_bind(ogs_sock_t *sock, ogs_sockaddr_t *addr)

```
....
115.      memcpy(&sock->local_addr, addr, sizeof(sock->local_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=398
Status	New

The size of the buffer used by ogs_sock_connect in ->, at line 122 of open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ogs_sock_connect passes to ->, at line 122 of open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c
Line	140	140
Object	->	->

Code Snippet

File Name	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c
Method	int ogs_sock_connect(ogs_sock_t *sock, ogs_sockaddr_t *addr)

```
....
140.      memcpy(&sock->remote_addr, addr, sizeof(sock->remote_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=399
Status	New

The size of the buffer used by *ogs_sock_accept in ->, at line 161 of open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ogs_sock_accept passes to ->, at line 161 of open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c
Line	186	186
Object	->	->

Code Snippet

File Name	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c
Method	ogs_sock_t *ogs_sock_accept(ogs_sock_t *sock)

```
....
186.      memcpy(&new_sock->remote_addr, &addr, sizeof(new_sock-
>remote_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=400
Status	New

The size of the buffer used by ogs_sock_bind in ->, at line 97 of open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ogs_sock_bind passes to ->, at line 97 of open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c
Line	115	115
Object	->	->

Code Snippet	
File Name	open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c
Method	int ogs_sock_bind(ogs_sock_t *sock, ogs_sockaddr_t *addr)

```
....
115.      memcpy(&sock->local_addr, addr, sizeof(sock->local_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=401
Status	New

The size of the buffer used by ogs_sock_connect in ->, at line 122 of open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ogs_sock_connect passes to ->, at line 122 of open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c
Line	140	140
Object	->	->

Code Snippet	
File Name	open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c
Method	int ogs_sock_connect(ogs_sock_t *sock, ogs_sockaddr_t *addr)

```
....
140.      memcpy(&sock->remote_addr, addr, sizeof(sock->remote_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=402
Status	New

The size of the buffer used by *ogs_sock_accept in ->, at line 161 of open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ogs_sock_accept passes to ->, at line 161 of open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c
Line	186	186

Object	->	->

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c
Method ogs_sock_t *ogs_sock_accept(ogs_sock_t *sock)

```
....
186.      memcpy(&new_sock->remote_addr, &addr, sizeof(new_sock-
>remote_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=403
Status	New

The size of the buffer used by upf_gtp_send_router_advertisement in src_ipsub, at line 495 of open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that upf_gtp_send_router_advertisement passes to src_ipsub, at line 495 of open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	543	543
Object	src_ipsub	src_ipsub

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static int upf_gtp_send_router_advertisement(

```
....
543.                  sizeof src_ipsub.sub);
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=404
Status	New

The size of the buffer used by upf_gtp_send_router_advertisement in prefix, at line 495 of open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that upf_gtp_send_router_advertisement passes to prefix, at line 495 of open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination

File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	561	561
Object	prefix	prefix

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static int upf_gtp_send_router_advertisement(

```
....
561.              subnet->sub.sub, sizeof prefix-
>nd_opt_pi_prefix.s6_addr);
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=405
Status	New

The size of the buffer used by upf_gtp_send_router_advertisement in src_ipsub, at line 495 of open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that upf_gtp_send_router_advertisement passes to src_ipsub, at line 495 of open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	567	567
Object	src_ipsub	src_ipsub

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static int upf_gtp_send_router_advertisement(

```
....
567.      memcpy(p, src_ipsub.sub, sizeof src_ipsub.sub);
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=406
Status	New

The size of the buffer used by upf_gtp_send_router_advertisement in src_ipsub, at line 495 of open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c, is not properly verified before writing data to the buffer.

This can enable a buffer overflow attack, using the source buffer that upf_gtp_send_router_advertisement passes to src_ipsub, at line 495 of open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	579	579
Object	src_ipsub	src_ipsub

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static int upf_gtp_send_router_advertisement(

```
....
579.      memcpy(ip6_h->ip6_src.s6_addr, src_ipsub.sub, sizeof
src_ipsub.sub);
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=407
Status New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 438 of open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 438 of open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Line	455	455
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
455.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=408

Status	New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 438 of open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 438 of open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Line	455	455
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Method static ogs_sbi_session_t *session_add(

```
....
455.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=409
Status	New

The size of the buffer used by *session_add in ogs_sockaddr_t, at line 442 of open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sockaddr_t, at line 442 of open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Line	459	459
Object	ogs_sockaddr_t	ogs_sockaddr_t

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
459.      memcpy(sbi_sess->addr, &sock->remote_addr,
sizeof(ogs_sockaddr_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=410
Status	New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 390 of open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 390 of open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Line	399	399
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
399.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=411
Status	New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 438 of open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 438 of open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Line	448	448
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
448.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=412
Status	New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 390 of open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 390 of open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Line	399	399
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
399.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=413
Status	New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 438 of open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 438 of open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Line	448	448
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Method static ogs_sbi_session_t *session_add(

```
....
448.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=414
Status	New

The size of the buffer used by *stream_add in ogs_sbi_stream_t, at line 394 of open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *stream_add passes to ogs_sbi_stream_t, at line 394 of open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Line	403	403
Object	ogs_sbi_stream_t	ogs_sbi_stream_t

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
403.      memset(stream, 0, sizeof(ogs_sbi_stream_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=415
Status	New

The size of the buffer used by *session_add in ogs_sbi_session_t, at line 442 of open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *session_add passes to ogs_sbi_session_t, at line 442 of open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c, to overwrite the target buffer.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Line	452	452
Object	ogs_sbi_session_t	ogs_sbi_session_t

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
452.      memset(sbi_sess, 0, sizeof(ogs_sbi_session_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=416
Status	New

The size of the buffer used by get_open_session_meta in ->, at line 314 of OP-TEE@@optee_os-3.10.0-CVE-2022-46152-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_open_session_meta passes to ->, at line 314 of OP-TEE@@optee_os-3.10.0-CVE-2022-46152-TP.c, to overwrite the target buffer.

	Source	Destination
File	OP-TEE@@optee_os-3.10.0-CVE-2022-46152-TP.c	OP-TEE@@optee_os-3.10.0-CVE-2022-46152-TP.c
Line	333	333
Object	->	->

Code Snippet
File Name OP-TEE@@optee_os-3.10.0-CVE-2022-46152-TP.c
Method static TEE_Result get_open_session_meta(size_t num_params,

```
....
333.              memset(&clnt_id->uuid, 0, sizeof(clnt_id->uuid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=417
Status	New

The size of the buffer used by get_open_session_meta in ->, at line 314 of OP-TEE@@optee_os-3.12.0-rc1-CVE-2022-46152-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_open_session_meta passes to ->, at line 314 of OP-TEE@@optee_os-3.12.0-rc1-CVE-2022-46152-FP.c, to overwrite the target buffer.

	Source	Destination
File	OP-TEE@@optee_os-3.12.0-rc1-CVE-2022-46152-FP.c	OP-TEE@@optee_os-3.12.0-rc1-CVE-2022-46152-FP.c
Line	333	333
Object	->	->

Code Snippet
File Name OP-TEE@@optee_os-3.12.0-rc1-CVE-2022-46152-FP.c
Method static TEE_Result get_open_session_meta(size_t num_params,

```
....
333.              memset(&clnt_id->uuid, 0, sizeof(clnt_id->uuid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=418
Status	New

The size of the buffer used by get_open_session_meta in ->, at line 314 of OP-TEE@@optee_os-3.13.0-rc1-CVE-2022-46152-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_open_session_meta passes to ->, at line 314 of OP-TEE@@optee_os-3.13.0-rc1-CVE-2022-46152-FP.c, to overwrite the target buffer.

	Source	Destination
File	OP-TEE@@optee_os-3.13.0-rc1-CVE-2022-46152-FP.c	OP-TEE@@optee_os-3.13.0-rc1-CVE-2022-46152-FP.c
Line	333	333
Object	->	->

Code Snippet
File Name OP-TEE@@optee_os-3.13.0-rc1-CVE-2022-46152-FP.c
Method static TEE_Result get_open_session_meta(size_t num_params,

```
....
333.              memset(&clnt_id->uuid, 0, sizeof(clnt_id->uuid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=419
Status	New

The size of the buffer used by get_open_session_meta in ->, at line 314 of OP-TEE@@optee_os-3.15.0-rc1-CVE-2022-46152-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_open_session_meta passes to ->, at line 314 of OP-TEE@@optee_os-3.15.0-rc1-CVE-2022-46152-TP.c, to overwrite the target buffer.

	Source	Destination
File	OP-TEE@@optee_os-3.15.0-rc1-CVE-2022-46152-TP.c	OP-TEE@@optee_os-3.15.0-rc1-CVE-2022-46152-TP.c
Line	333	333
Object	->	->

Code Snippet
File Name OP-TEE@@optee_os-3.15.0-rc1-CVE-2022-46152-TP.c
Method static TEE_Result get_open_session_meta(size_t num_params,

```
....
333.              memset(&clnt_id->uuid, 0, sizeof(clnt_id->uuid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=420
Status	New

The size of the buffer used by get_open_session_meta in ->, at line 315 of OP-TEE@@optee_os-3.16.0-rc1-CVE-2022-46152-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_open_session_meta passes to ->, at line 315 of OP-TEE@@optee_os-3.16.0-rc1-CVE-2022-46152-TP.c, to overwrite the target buffer.

	Source	Destination
File	OP-TEE@@optee_os-3.16.0-rc1-CVE-2022-46152-TP.c	OP-TEE@@optee_os-3.16.0-rc1-CVE-2022-46152-TP.c
Line	334	334
Object	->	->

Code Snippet
File Name OP-TEE@@optee_os-3.16.0-rc1-CVE-2022-46152-TP.c
Method static TEE_Result get_open_session_meta(size_t num_params,

```
....
334.              memset(&clnt_id->uuid, 0, sizeof(clnt_id->uuid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=421
Status	New

The size of the buffer used by get_open_session_meta in ->, at line 315 of OP-TEE@@optee_os-3.18.0-rc1-CVE-2022-46152-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_open_session_meta passes to ->, at line 315 of OP-TEE@@optee_os-3.18.0-rc1-CVE-2022-46152-FP.c, to overwrite the target buffer.

	Source	Destination
File	OP-TEE@@optee_os-3.18.0-rc1-CVE-2022-46152-FP.c	OP-TEE@@optee_os-3.18.0-rc1-CVE-2022-46152-FP.c
Line	334	334
Object	->	->

Code Snippet
File Name OP-TEE@@optee_os-3.18.0-rc1-CVE-2022-46152-FP.c

Method	static TEE_Result get_open_session_meta(size_t num_params, ``` .... 334. memset(&clnt_id->uuid, 0, sizeof(clnt_id->uuid)); ```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=422
Status	New

The size of the buffer used by get_open_session_meta in ->, at line 263 of OP-TEE@@optee_os-3.8.0-rc1-CVE-2022-46152-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_open_session_meta passes to ->, at line 263 of OP-TEE@@optee_os-3.8.0-rc1-CVE-2022-46152-TP.c, to overwrite the target buffer.

	Source	Destination
File	OP-TEE@@optee_os-3.8.0-rc1-CVE-2022-46152-TP.c	OP-TEE@@optee_os-3.8.0-rc1-CVE-2022-46152-TP.c
Line	281	281
Object	->	->

Code Snippet	
File Name	OP-TEE@@optee_os-3.8.0-rc1-CVE-2022-46152-TP.c
Method	static TEE_Result get_open_session_meta(size_t num_params, ``` .... 281. memset(&clnt_id->uuid, 0, sizeof(clnt_id->uuid)); ```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=423
Status	New

The size of the buffer used by get_open_session_meta in ->, at line 265 of OP-TEE@@optee_os-3.9.0-rc1-CVE-2022-46152-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_open_session_meta passes to ->, at line 265 of OP-TEE@@optee_os-3.9.0-rc1-CVE-2022-46152-FP.c, to overwrite the target buffer.

	Source	Destination
File	OP-TEE@@optee_os-3.9.0-rc1-CVE-2022-46152-FP.c	OP-TEE@@optee_os-3.9.0-rc1-CVE-2022-46152-FP.c
Line	284	284
Object	->	->

Code Snippet

File Name	OP-TEE@@optee_os-3.9.0-rc1-CVE-2022-46152-FP.c
Method	static TEE_Result get_open_session_meta(size_t num_params,

```
....
284.              memset(&clnt_id->uuid, 0, sizeof(clnt_id->uuid));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=424
Status	New

The size of the buffer used by mbedtls_rsa_init in mbedtls_rsa_context, at line 456 of OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mbedtls_rsa_init passes to mbedtls_rsa_context, at line 456 of OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c, to overwrite the target buffer.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	458	458
Object	mbedtls_rsa_context	mbedtls_rsa_context

Code Snippet

File Name	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method	void mbedtls_rsa_init(mbedtls_rsa_context *ctx)

```
....
458.      memset(ctx, 0, sizeof(mbedtls_rsa_context));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=425
Status	New

The size of the buffer used by mbedtls_rsa_init in mbedtls_rsa_context, at line 456 of OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mbedtls_rsa_init passes to mbedtls_rsa_context, at line 456 of OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c, to overwrite the target buffer.

	Source	Destination
File	OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c
Line	458	458
Object	mbedtls_rsa_context	mbedtls_rsa_context

Code Snippet
File Name OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c
Method void mbedtls_rsa_init(mbedtls_rsa_context *ctx)

```
....
458.      memset(ctx, 0, sizeof(mbedtls_rsa_context));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=426
Status New

The size of the buffer used by foveon_interpolate in black, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that foveon_interpolate passes to black, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3116	3116
Object	black	black

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3116.    memcpy (black, black+8, sizeof *black*8);
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=427
Status New

The size of the buffer used by foveon_interpolate in black, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that foveon_interpolate passes to black, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3117	3117
Object	black	black

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS foveon_interpolate()

```
....
3117.    memcpy (black+height-11, black+height-22, 11*sizeof *black);
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=428
Status	New

The size of the buffer used by foveon_interpolate in width, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that foveon_interpolate passes to width, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3368	3368
Object	width	width

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS foveon_interpolate()

```
....
3368.        memcpy (smrow[2], smrow[1], sizeof **smrow * width);
```

Buffer Overflow Loops

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow Loops\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=500
Status	New

The buffer allocated by c in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 972 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	975	1033
Object	0	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS canon_sraw_load_raw()

```
....
975.    short *rp=0, (*ip)[4];
....
1033.       FORC3 rp[c] = CLIP(pix[c] * sraw_mul[c] >> 10);
```

Buffer Overflow Loops\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=501
Status New

The buffer allocated by c in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 2495 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2499	2507
Object	0	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_rgb_load_raw()

```
....
2499.    ushort *ip=image[0];
....
2507.       FORC3 if ((ip[c] = rgb[c] += *bp++) >> 12) derror();
```

Buffer Overflow Loops\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=502

Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3109
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3109.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=503
Status	New

The buffer allocated by ddft in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3055
Object	2	ddft

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3055.        FORC3 ddft[i+1][c][1] /= (dstb[3]-dstb[1]+1) * (dstb[2]-
dstb[0]+1);
```

Buffer Overflow Loops\Path 5:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=504
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3109
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3109.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=505
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3110
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3110.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=506
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3110
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3110.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=507
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3155
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3155.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=508
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3155
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3155.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=509
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3156
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3156.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=510
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3156
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3156.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=511
Status	New

The buffer allocated by c in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3170
Object	2	c

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3170.              - ddft[0][c][1] - ddft[0][c][0] * ((float) col/width -
0.5)
```

Buffer Overflow Loops\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=512
Status	New

The buffer allocated by c in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3170
Object	2	c

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3170.              - ddft[0][c][1] - ddft[0][c][0] * ((float) col/width -
0.5)
```

Buffer Overflow Loops\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=513
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3109

Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3109.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=514
Status	New

The buffer allocated by ddft in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3055
Object	3	ddft

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3055.        FORC3 ddft[i+1][c][1] /= (dstb[3]-dstb[1]+1) * (dstb[2]-
dstb[0]+1);
```

Buffer Overflow Loops\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=515
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3109
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3109.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=516
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3110
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3110.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=517
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3110
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3110.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=518
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3155
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3155.         ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=519
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3155
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3155.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=520
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3156
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3156.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=521

Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3156
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3156.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=522
Status	New

The buffer allocated by c in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3170
Object	3	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3170.              - ddft[0][c][1] - ddft[0][c][0] * ((float) col/width -
0.5)
```

Buffer Overflow Loops\Path 24:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=523
Status	New

The buffer allocated by c in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3170
Object	3	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3170.              - ddft[0][c][1] - ddft[0][c][0] * ((float) col/width -
0.5)
```

Buffer Overflow Loops\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=524
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3109
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3109.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=525
Status	New

The buffer allocated by ddft in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3055
Object	3	ddft

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3055.        FORC3 ddft[i+1][c][1] /= (dstb[3]-dstb[1]+1) * (dstb[2]-
dstb[0]+1);
```

Buffer Overflow Loops\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=526
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3109
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3109.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=527
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3110
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3110.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=528
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3110
Object	3	i

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3110.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=529
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3155
Object	3	i

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3155.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=530
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3155
Object	3	i

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3155.        ddft[0][0][i] = ddft[1][0][i] +
```

Buffer Overflow Loops\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=531
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3156
Object	3	i

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3156.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=532
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Line	3018	3156
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3156.        row / (height-1.0) * (ddft[2][0][i] - ddft[1][0][i]);
```

Buffer Overflow Loops\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=533
Status New

The buffer allocated by c in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3170
Object	3	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3170.              - ddft[0][c][1] - ddft[0][c][0] * ((float) col/width -
0.5)
```

Buffer Overflow Loops\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=534
Status New

The buffer allocated by c in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3014 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3018	3170
Object	3	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3018.    float cfilt=0, ddft[3][3][2], ppm[3][3][3];
....
3170.              - ddft[0][c][1] - ddft[0][c][0] * ((float) col/width -
0.5)
```

Buffer Overflow Loops\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=535
Status New

The buffer allocated by gmb_cam in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3639
Object	4	gmb_cam

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3639.      FORCC gmb_cam[sq][c] = gmb_cam[sq][c]/count[c] - black;
```

Buffer Overflow Loops\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=536
Status New

The buffer allocated by gmb_cam in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3636
Object	4	gmb_cam

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3636.       gmb_cam[sq][c] += BAYER(row,col);
```

Buffer Overflow Loops\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=537
Status New

The buffer allocated by sq in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3639
Object	4	sq

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3639.      FORCC gmb_cam[sq][c] = gmb_cam[sq][c]/count[c] - black;
```

Buffer Overflow Loops\Path 39:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=538
Status	New

The buffer allocated by k in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3649
Object	4	k

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3649.       cam_xyz[i][j] += gmb_cam[k][i] * inverse[k][j];
```

Buffer Overflow Loops\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=539
Status	New

The buffer allocated by gmb_cam in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3639
Object	24	gmb_cam

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3639.      FORCC gmb_cam[sq][c] = gmb_cam[sq][c]/count[c] - black;
```

Buffer Overflow Loops\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=540
Status	New

The buffer allocated by gmb_cam in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3636
Object	24	gmb_cam

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3636.        gmb_cam[sq][c] += BAYER(row,col);
```

Buffer Overflow Loops\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=541
Status	New

The buffer allocated by sq in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3639
Object	24	sq

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3639.      FORCC gmb_cam[sq][c] = gmb_cam[sq][c]/count[c] - black;
```

Buffer Overflow Loops\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=542
Status	New

The buffer allocated by k in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3649
Object	24	k

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3649.        cam_xyz[i][j] += gmb_cam[k][i] * inverse[k][j];
```

Buffer Overflow Loops\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=543
Status	New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3641
Object	3	gmb_xyz

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3641.      gmb_xyz[sq][1] = gmb_xyY[sq][2];
```

Buffer Overflow Loops\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=544
Status	New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3640
Object	3	gmb_xyz

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3640.      gmb_xyz[sq][0] = gmb_xyY[sq][2] * gmb_xyY[sq][0] /
gmb_xyY[sq][1];
```

Buffer Overflow Loops\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=545
Status	New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3642

Object	3	gmb_xyz

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3642.      gmb_xyz[sq][2] = gmb_xyY[sq][2] *
```

Buffer Overflow Loops\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=546
Status New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3641
Object	24	gmb_xyz

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3641.      gmb_xyz[sq][1] = gmb_xyY[sq][2];
```

Buffer Overflow Loops\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=547
Status New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-	ONLYOFFICE@@core-v5.5.99.2024-CVE-

	2022-29776-FP.c	2022-29776-FP.c
Line	3625	3640
Object	24	gmb_xyz

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3640.      gmb_xyz[sq][0] = gmb_xyY[sq][2] * gmb_xyY[sq][0] /
gmb_xyY[sq][1];
```

Buffer Overflow Loops\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=548
Status New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3625	3642
Object	24	gmb_xyz

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3625.    double gmb_cam[NSQ][4], gmb_xyz[NSQ][3];
....
3642.      gmb_xyz[sq][2] = gmb_xyY[sq][2] *
```

Buffer Overflow Loops\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=549
Status New

The buffer allocated by k in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3569 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3626	3649
Object	3	k

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS colorcheck()

```
....
3626.    double inverse[NSQ][3], cam_xyz[4][3], num;
....
3649.       cam_xyz[i][j] += gmb_cam[k][i] * inverse[k][j];
```

Stored Buffer Overflow boundcpy

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow boundcpy Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description
Stored Buffer Overflow boundcpy\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2138
Status	New

The size of the buffer used by ljpeg_start in Pointer, at line 823 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	Pointer

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2139
Status	New

The size of the buffer used by ljpeg_start in jh, at line 823 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	jh

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2140
Status	New

The size of the buffer used by ljpeg_start in sizeof, at line 823 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2141
Status New

The size of the buffer used by canon_compressed_load_raw in diffbuf, at line 737 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	758
Object	fgetc	diffbuf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS canon_compressed_load_raw()

```
....
758.        memset (diffbuf, 0, sizeof diffbuf);
```

Stored Buffer Overflow boundcpy\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2142
Status	New

The size of the buffer used by canon_compressed_load_raw in sizeof, at line 737 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	758
Object	fgetc	sizeof

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS canon_compressed_load_raw()

```
....
758.        memset (diffbuf, 0, sizeof diffbuf);
```

Stored Buffer Overflow boundcpy\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2143
Status	New

The size of the buffer used by kodak_radc_load_raw in buf, at line 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable

a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	buf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2144
Status New

The size of the buffer used by kodak_radc_load_raw in sizeof, at line 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2145
Status	New

The size of the buffer used by kodak_radc_load_raw in BinaryExpr, at line 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	BinaryExpr

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2146
Status	New

The size of the buffer used by kodak_radc_load_raw in sizeof, at line 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable

a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2147
Status New

The size of the buffer used by kodak_radc_load_raw in c, at line 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2148
Status	New

The size of the buffer used by kodak_radc_load_raw in c, at line 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	c

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2149
Status	New

The size of the buffer used by kodak_radc_load_raw in BinaryExpr, at line 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable

a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2150
Status New

The size of the buffer used by kodak_radc_load_raw in buf, at line 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	buf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2151
Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that kodak_65000_decode passes to fgetc, at line 2406 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2416	2505
Object	fgetc	rgb

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2416.       c = fgetc(ifp);
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS kodak_rgb_load_raw()

```
....
2505.         memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2152
Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable

a buffer overflow attack, using the source buffer that kodak_65000_decode passes to fgetc, at line 2406 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2432	2505
Object	fgetc	rgb

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2432.      bitbuf += fgetc(ifp);
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2153
Status New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_shorts passes to pixel, at line 342 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	344	2505
Object	pixel	rgb

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS read_shorts (ushort *pixel, int count)

```
....
344.    if (fread (pixel, 2, count, ifp) < count) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2154
Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that kodak_65000_decode passes to fgetc, at line 2406 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2416	2505
Object	fgetc	sizeof

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2416.      c = fgetc(ifp);
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2155
Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable

a buffer overflow attack, using the source buffer that kodak_65000_decode passes to fgetc, at line 2406 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2432	2505
Object	fgetc	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2432.      bitbuf += fgetc(ifp);
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2156
Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_shorts passes to pixel, at line 342 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	344	2505
Object	pixel	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS read_shorts (ushort *pixel, int count)

```
....
344.    if (fread (pixel, 2, count, ifp) < count) derror();
```

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2157
Status	New

The size of the buffer used by kodak_radc_load_raw in buf, at line 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	buf

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2158
Status	New

The size of the buffer used by kodak_radc_load_raw in sizeof, at line 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can

enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2159
Status New

The size of the buffer used by kodak_radc_load_raw in BinaryExpr, at line 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2160
Status	New

The size of the buffer used by kodak_radc_load_raw in sizeof, at line 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	sizeof

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2161
Status	New

The size of the buffer used by kodak_radc_load_raw in c, at line 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can

enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	c

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2162
Status New

The size of the buffer used by kodak_radc_load_raw in c, at line 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	c

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2163
Status	New

The size of the buffer used by kodak_radc_load_raw in BinaryExpr, at line 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	BinaryExpr

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2164
Status	New

The size of the buffer used by kodak_radc_load_raw in buf, at line 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can

enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	buf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2214.       memcpy (buf[c][0]+!c, buf[c][2], sizeof buf[c][0]-2*!c);
```

Stored Buffer Overflow boundcpy\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2165
Status New

The size of the buffer used by ljpeg_start in Pointer, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	Pointer

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2166
Status	New

The size of the buffer used by ljpeg_start in Pointer, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ljpeg_start passes to data, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	832	829
Object	data	Pointer

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
832.    fread (data, 2, 1, ifp);
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2167
Status	New

The size of the buffer used by ljpeg_start in Pointer, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ljpeg_start passes to data, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	835	829

Object	data	Pointer

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
835.      fread (data, 2, 2, ifp);
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2168
Status New

The size of the buffer used by ljpeg_start in Pointer, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ljpeg_start passes to data, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	839	829
Object	data	Pointer

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
839.      fread (data, 1, len, ifp);
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2169
Status New

The size of the buffer used by ljpeg_start in jh, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	jh

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2170
Status	New

The size of the buffer used by ljpeg_start in jh, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ljpeg_start passes to data, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	832	829
Object	data	jh

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
832.    fread (data, 2, 1, ifp);
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2171
Status	New

The size of the buffer used by ljpeg_start in jh, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ljpeg_start passes to data, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	835	829
Object	data	jh

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
835.      fread (data, 2, 2, ifp);
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2172
Status	New

The size of the buffer used by ljpeg_start in jh, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ljpeg_start passes to data, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	839	829
Object	data	jh

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
839.      fread (data, 1, len, ifp);
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2173
Status	New

The size of the buffer used by ljpeg_start in sizeof, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2174
Status	New

The size of the buffer used by ljpeg_start in sizeof, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ljpeg_start passes to data, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	832	829
Object	data	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
832.    fread (data, 2, 1, ifp);
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2175
Status New

The size of the buffer used by ljpeg_start in sizeof, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ljpeg_start passes to data, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	835	829
Object	data	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
835.      fread (data, 2, 2, ifp);
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2176
Status New

The size of the buffer used by ljpeg_start in sizeof, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ljpeg_start passes to data, at line 823 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	839	829
Object	data	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
839.      fread (data, 1, len, ifp);
....
829.    memset (jh, 0, sizeof *jh);
```

Stored Buffer Overflow boundcpy\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2177
Status New

The size of the buffer used by canon_compressed_load_raw in diffbuf, at line 737 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	758
Object	fgetc	diffbuf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS canon_compressed_load_raw()

```
....
758.        memset (diffbuf, 0, sizeof diffbuf);
```

Stored Buffer Overflow boundcpy\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2178
Status	New

The size of the buffer used by canon_compressed_load_raw in sizeof, at line 737 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getbits passes to fgetc, at line 575 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	585	758
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method void CLASS canon_compressed_load_raw()

```
....
758.        memset (diffbuf, 0, sizeof diffbuf);
```

Stored Buffer Overflow boundcpy\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2179
Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that kodak_65000_decode passes to fgetc, at line 2406 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

Source	Destination

File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2416	2505
Object	fgetc	rgb

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2416.       c = fgetc(ifp);
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.         memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2180
Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that kodak_65000_decode passes to fgetc, at line 2406 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2432	2505
Object	fgetc	rgb

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2432.       bitbuf += fgetc(ifp);
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2181
Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_shorts passes to pixel, at line 342 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	344	2505
Object	pixel	rgb

Code Snippet

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method void CLASS read_shorts (ushort *pixel, int count)

```
....
344.    if (fread (pixel, 2, count, ifp) < count) derror();
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2182
Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that kodak_65000_decode passes to fgetc, at line 2406 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination

File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2416	2505
Object	fgetc	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2416.       c = fgetc(ifp);
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.         memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2183
Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that kodak_65000_decode passes to fgetc, at line 2406 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2432	2505
Object	fgetc	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2432.       bitbuf += fgetc(ifp);
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2184
Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_shorts passes to pixel, at line 342 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	344	2505
Object	pixel	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method void CLASS read_shorts (ushort *pixel, int count)

```
....
344.    if (fread (pixel, 2, count, ifp) < count) derror();
```

File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Use of Zero Initialized Pointer

Query Path:

CPP\Cx\CPP Medium Threat\Use of Zero Initialized Pointer Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Zero Initialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2101

Status	New

The variable declared in sock at open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c in line 53 is not initialized when it is used by sock at open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c in line 53.

	Source	Destination
File	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c	open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c
Line	55	57
Object	sock	sock

Code Snippet
File Name open5gs@@open5gs-v1.2.2-CVE-2021-44109-FP.c
Method ogs_sock_t *ogs_sock_create(void)

```
....
55.      ogs_sock_t *sock = NULL;
....
57.      sock = ogs_calloc(1, sizeof(*sock));
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2102
Status	New

The variable declared in context at open5gs@@open5gs-v1.2.2-CVE-2023-50020-FP.c in line 54 is not initialized when it is used by context at open5gs@@open5gs-v1.2.2-CVE-2023-50020-FP.c in line 54.

	Source	Destination
File	open5gs@@open5gs-v1.2.2-CVE-2023-50020-FP.c	open5gs@@open5gs-v1.2.2-CVE-2023-50020-FP.c
Line	56	59
Object	context	context

Code Snippet
File Name open5gs@@open5gs-v1.2.2-CVE-2023-50020-FP.c
Method static void epoll_init(ogs_pollset_t *pollset)

```
....
56.      struct epoll_context_s *context = NULL;
....
59.      context = ogs_calloc(1, sizeof *context);
```

Use of Zero Initialized Pointer\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2103
Status	New

The variable declared in sock at open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c in line 53 is not initialized when it is used by sock at open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c in line 53.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c
Line	55	57
Object	sock	sock

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-44109-FP.c
Method ogs_sock_t *ogs_sock_create(void)

```
....
55.      ogs_sock_t *sock = NULL;
....
57.      sock = ogs_calloc(1, sizeof(*sock));
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2104
Status	New

The variable declared in ip6_h at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 495 is not initialized when it is used by ip6_h at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 495.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	511	530
Object	ip6_h	ip6_h

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static int upf_gtp_send_router_advertisement(

```
....
511.      struct ip6_hdr *ip6_h =  NULL;
....
530.      pkbuf->len = sizeof *ip6_h + sizeof *advert_h + sizeof
*prefix;
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2105
Status	New

The variable declared in advert_h at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 495 is not initialized when it is used by advert_h at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 495.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	512	530
Object	advert_h	advert_h

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static int upf_gtp_send_router_advertisement(

```
....
512.      struct nd_router_advert *advert_h = NULL;
....
530.      pkbuf->len = sizeof *ip6_h + sizeof *advert_h + sizeof
*prefix;
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2106
Status	New

The variable declared in prefix at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 495 is not initialized when it is used by prefix at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 495.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	513	530
Object	prefix	prefix

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static int upf_gtp_send_router_advertisement(

```
....
513.      struct nd_opt_prefix_info *prefix = NULL;
....
530.      pkbuf->len = sizeof *ip6_h + sizeof *advert_h + sizeof
*prefix;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2107
Status	New

The variable declared in subnet at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 84 is not initialized when it is used by subnet at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 84.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	99	233
Object	subnet	subnet

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static void _gtpv1_u_recv_cb(short when, ogs_socket_t fd, void *data)

```
....
99.      ogs_pfcp_subnet_t *subnet = NULL;
....
233.      dev = subnet->dev;
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2108
Status	New

The variable declared in dev at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 242 is not initialized when it is used by dev at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 242.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	244	278
Object	dev	dev

Code Snippet	
File Name	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method	int upf_gtp_open(void)

```
....
244.      ogs_pfcp_dev_t *dev = NULL;
....
278.          dev->fd = ogs_tun_open(dev->ifname, OGS_MAX_IFNAME_LEN,
0);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2109
Status	New

The variable declared in subnet at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 242 is not initialized when it is used by subnet at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 242.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	245	301
Object	subnet	subnet

Code Snippet	
File Name	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method	int upf_gtp_open(void)

```
....
245.      ogs_pfcp_subnet_t *subnet = NULL;
....
301.          ogs_assert(subnet->dev);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2110
Status	New

The variable declared in node at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 242 is not initialized when it is used by sock at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 242.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c

Line	246	251
Object	node	sock

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
246.      ogs_socknode_t *node = NULL;
....
251.          sock = ogs_gtp_server(node);
```

Use of Zero Initialized Pointer\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2111
Status New

The variable declared in dev at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316 is not initialized when it is used by dev at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	318	325
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
318.      ogs_pfcp_dev_t *dev = NULL;
....
325.          ogs_closesocket(dev->fd);
```

Use of Zero Initialized Pointer\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2112
Status New

The variable declared in dev at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316 is not initialized when it is used by dev at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316.

	Source	Destination

File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	318	324
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
318.      ogs_pfcp_dev_t *dev = NULL;
....
324.              ogs_pollset_remove(dev->poll);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2113
Status	New

The variable declared in dev at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316 is not initialized when it is used by dev at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	318	323
Object	dev	dev

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
318.      ogs_pfcp_dev_t *dev = NULL;
....
323.          if (dev->poll)
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2114
Status	New

The variable declared in sess at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 428 is not initialized when it is used by pdr at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 428.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	445	453
Object	sess	pdr

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static int upf_gtp_handle_multicast(ogs_pkbuf_t *recvbuf)

```
....
445.              upf_sess_t *sess = NULL;
....
453.                      pdr = ogs_pfcp_sess_default_pdr(&sess->pfcp);
```

Use of Zero Initialized Pointer\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2115
Status New

The variable declared in sess at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 428 is not initialized when it is used by sess at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 428.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	445	449
Object	sess	sess

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static int upf_gtp_handle_multicast(ogs_pkbuf_t *recvbuf)

```
....
445.              upf_sess_t *sess = NULL;
....
449.                  if (sess->ipv6) {
```

Use of Zero Initialized Pointer\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2116
Status New

The variable declared in context at open5gs@@open5gs-v1.3.0-CVE-2023-50020-FP.c in line 60 is not initialized when it is used by context at open5gs@@open5gs-v1.3.0-CVE-2023-50020-FP.c in line 60.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2023-50020-FP.c	open5gs@@open5gs-v1.3.0-CVE-2023-50020-FP.c
Line	62	65
Object	context	context

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2023-50020-FP.c
Method static void epoll_init(ogs_pollset_t *pollset)

```
....
62.      struct epoll_context_s *context = NULL;
....
65.      context = ogs_calloc(1, sizeof *context);
```

Use of Zero Initialized Pointer\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2117
Status New

The variable declared in node at open5gs@@open5gs-v2.0.22-CVE-2021-45462-FP.c in line 198 is not initialized when it is used by sock at open5gs@@open5gs-v2.0.22-CVE-2021-45462-FP.c in line 198.

	Source	Destination
File	open5gs@@open5gs-v2.0.22-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.0.22-CVE-2021-45462-FP.c
Line	200	204
Object	node	sock

Code Snippet
File Name open5gs@@open5gs-v2.0.22-CVE-2021-45462-FP.c
Method int sgwu_gtp_open(void)

```
....
200.      ogs_socknode_t *node = NULL;
....
204.          sock = ogs_gtp_server(node);
```

Use of Zero Initialized Pointer\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2118

Status	New

The variable declared in context at open5gs@@open5gs-v2.0.22-CVE-2023-50020-FP.c in line 60 is not initialized when it is used by context at open5gs@@open5gs-v2.0.22-CVE-2023-50020-FP.c in line 60.

	Source	Destination
File	open5gs@@open5gs-v2.0.22-CVE-2023-50020-FP.c	open5gs@@open5gs-v2.0.22-CVE-2023-50020-FP.c
Line	62	65
Object	context	context

Code Snippet
File Name open5gs@@open5gs-v2.0.22-CVE-2023-50020-FP.c
Method static void epoll_init(ogs_pollset_t *pollset)

```
....
62.      struct epoll_context_s *context = NULL;
....
65.      context = ogs_calloc(1, sizeof *context);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2119
Status	New

The variable declared in stream at open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c in line 390 is not initialized when it is used by stream at open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c in line 1053.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Line	393	1068
Object	stream	stream

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
393.      ogs_sbi_stream_t *stream = NULL;
```

File Name open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Method static int on_begin_headers(nghttp2_session *session,

```
....
1068.       stream = stream_add(sbi_sess, frame->hd.stream_id);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2120
Status	New

The variable declared in sbi_sess at open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c in line 438 is not initialized when it is used by sbi_sess at open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c in line 506.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Line	441	535
Object	sbi_sess	sbi_sess

Code Snippet

File Name open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c

Method static ogs_sbi_session_t *session_add(

```
....
441.       ogs_sbi_session_t *sbi_sess = NULL;
```

File Name open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c

Method static void accept_handler(short when, ogs_socket_t fd, void *data)

```
....
535.       sbi_sess = session_add(server, new);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2121
Status	New

The variable declared in saveptr at open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c in line 814 is not initialized when it is used by request at open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c in line 814.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c

Line	865	871
Object	saveptr	request

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Method static int on_header(nghttp2_session *session, const nghttp2_frame *frame,

```
....
865.          char *saveptr = NULL, *query;
....
871.          request->h.uri = ogs_sbi_parse_uri(valuestr, "?",
&saveptr);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2122
Status	New

The variable declared in data at open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c in line 1182 is not initialized when it is used by pkbuf at open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c in line 1182.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Line	1195	1209
Object	data	pkbuf

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2021-44109-FP.c
Method static int session_send(ogs_sbi_session_t *sbi_sess)

```
....
1195.          const uint8_t *data = NULL;
....
1209.          pkbuf = ogs_pkbuf_alloc(NULL, data_len);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2123
Status	New

The variable declared in node at open5gs@@open5gs-v2.2.0-CVE-2021-45462-FP.c in line 198 is not initialized when it is used by sock at open5gs@@open5gs-v2.2.0-CVE-2021-45462-FP.c in line 198.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v2.2.0-CVE-2021-45462-FP.c
Line	200	204
Object	node	sock

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2021-45462-FP.c
Method int sgwu_gtp_open(void)

```
....
200.      ogs_socknode_t *node = NULL;
....
204.          sock = ogs_gtp_server(node);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2124
Status	New

The variable declared in stream at open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c in line 390 is not initialized when it is used by stream at open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c in line 1053.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Line	393	1068
Object	stream	stream

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
393.      ogs_sbi_stream_t *stream = NULL;
```

File Name open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Method static int on_begin_headers(nghttp2_session *session,

```
....
1068.       stream = stream_add(sbi_sess, frame->hd.stream_id);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2125
Status	New

The variable declared in sbi_sess at open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c in line 438 is not initialized when it is used by sbi_sess at open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c in line 506.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Line	441	535
Object	sbi_sess	sbi_sess

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Method static ogs_sbi_session_t *session_add(

```
....
441.      ogs_sbi_session_t *sbi_sess = NULL;
```

File Name open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Method static void accept_handler(short when, ogs_socket_t fd, void *data)

```
....
535.      sbi_sess = session_add(server, new);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2126
Status	New

The variable declared in saveptr at open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c in line 814 is not initialized when it is used by request at open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c in line 814.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Line	865	871
Object	saveptr	request

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Method static int on_header(nghttp2_session *session, const nghttp2_frame *frame,

```
....
865.          char *saveptr = NULL, *query;
....
871.          request->h.uri = ogs_sbi_parse_uri(valuestr, "?",
&saveptr);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2127
Status	New

The variable declared in data at open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c in line 1182 is not initialized when it is used by pkbuf at open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c in line 1182.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c	open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Line	1195	1209
Object	data	pkbuf

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2022-3299-TP.c
Method static int session_send(ogs_sbi_session_t *sbi_sess)

```
....
1195.          const uint8_t *data = NULL;
....
1209.          pkbuf = ogs_pkbuf_alloc(NULL, data_len);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2128
Status	New

The variable declared in context at open5gs@@open5gs-v2.2.0-CVE-2023-50020-FP.c in line 60 is not initialized when it is used by context at open5gs@@open5gs-v2.2.0-CVE-2023-50020-FP.c in line 60.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2023-50020-FP.c	open5gs@@open5gs-v2.2.0-CVE-2023-50020-FP.c
Line	62	65
Object	context	context

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2023-50020-FP.c
Method static void epoll_init(ogs_pollset_t *pollset)

```
....
62.      struct epoll_context_s *context = NULL;
....
65.      context = ogs_calloc(1, sizeof *context);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2129
Status	New

The variable declared in stream at open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c in line 394 is not initialized when it is used by stream at open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c in line 1056.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Line	397	1071
Object	stream	stream

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Method static ogs_sbi_stream_t *stream_add(

```
....
397.      ogs_sbi_stream_t *stream = NULL;
```

File Name open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Method static int on_begin_headers(nghttp2_session *session,

```
....
1071.      stream = stream_add(sbi_sess, frame->hd.stream_id);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2130
Status	New

The variable declared in sbi_sess at open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c in line 442 is not initialized when it is used by sbi_sess at open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c in line 507.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Line	445	536
Object	sbi_sess	sbi_sess

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Method static ogs_sbi_session_t *session_add(

```
....
445.      ogs_sbi_session_t *sbi_sess = NULL;
```

File Name open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Method static void accept_handler(short when, ogs_socket_t fd, void *data)

```
....
536.      sbi_sess = session_add(server, new);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2131
Status	New

The variable declared in saveptr at open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c in line 816 is not initialized when it is used by request at open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c in line 816.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Line	867	873
Object	saveptr	request

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Method static int on_header(nghttp2_session *session, const nghttp2_frame *frame,

```
....
867.          char *saveptr = NULL, *query;
....
873.          request->h.uri = ogs_sbi_parse_uri(valuestr, "?",
&saveptr);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2132
Status	New

The variable declared in data at open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c in line 1185 is not initialized when it is used by pkbuf at open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c in line 1185.

	Source	Destination
File	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c	open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Line	1198	1212
Object	data	pkbuf

Code Snippet
File Name open5gs@@open5gs-v2.3.1-CVE-2021-44109-FP.c
Method static int session_send(ogs_sbi_session_t *sbi_sess)

```
....
1198.           const uint8_t *data = NULL;
....
1212.           pkbuf = ogs_pkbuf_alloc(NULL, data_len);
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2133
Status	New

The variable declared in pData at ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c in line 781 is not initialized when it is used by pData at ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c in line 781.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Line	783	788
Object	pData	pData

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Method std::string CUtf8Converter::GetUtf8StringFromUnicode2(const wchar_t* pUnicodes, LONG lCount, bool bIsBOM)

```
....
783.          BYTE* pData = NULL;
....
788.          std::string s((char*)pData, lLen);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2134
Status	New

The variable declared in pData at ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c in line 781 is not initialized when it is used by pData at ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c in line 781.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c
Line	783	788
Object	pData	pData

Code Snippet

File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c

Method std::string CUtf8Converter::GetUtf8StringFromUnicode2(const wchar_t* pUnicodes, LONG lCount, bool bIsBOM)

```
....
783.          BYTE* pData = NULL;
....
788.          std::string s((char*)pData, lLen);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2135
Status	New

The variable declared in pData at ONLYOFFICE@@core-v7.0.0.27-CVE-2022-29776-FP.c in line 781 is not initialized when it is used by pData at ONLYOFFICE@@core-v7.0.0.27-CVE-2022-29776-FP.c in line 781.

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2022-29776-FP.c
Line	783	788
Object	pData	pData

Code Snippet	
File Name	ONLYOFFICE@@core-v7.0.0.27-CVE-2022-29776-FP.c
Method	std::string CUtf8Converter::GetUtf8StringFromUnicode2(const wchar_t* pUnicodes, LONG lCount, bool bIsBOM)

```
....
783.          BYTE* pData = NULL;
....
788.          std::string s((char*)pData, lLen);
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2136
Status	New

The variable declared in rng_state at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2412 is not initialized when it is used by rng_state at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2412.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2418	2412
Object	rng_state	rng_state

Code Snippet	
File Name	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method	static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2418.          rng_state  = NULL;
....
2412.  static int myrand(void *rng_state, unsigned char *output, size_t
len)
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2137
Status	New

The variable declared in rng_state at OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c in line 2412 is not initialized when it is used by rng_state at OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c in line 2412.

	Source	Destination
File	OP-TEE@@optee_os-4.1.0-CVE-2024-	OP-TEE@@optee_os-4.1.0-CVE-2024-

	23170-TP.c	23170-TP.c
Line	2418	2412
Object	rng_state	rng_state

Code Snippet
File Name OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2418.          rng_state  = NULL;
....
2412.  static int myrand(void *rng_state, unsigned char *output, size_t
len)
```

Uncontrolled Recursion

Query Path:
CPP\Cx\CPP Medium Threat\Uncontrolled Recursion Version:1

Description

Uncontrolled Recursion\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2673
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2674
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-	ONLYOFFICE@@core-v5.5.2.2-CVE-

	2023-50980-TP.c	2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2675
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2676
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2023-50980-TP.c
Method	void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2677
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet

File Name	ONLYOFFICE@@core-v6.3.0.70-CVE-2023-50980-TP.c
Method	void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2678
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet

File Name	ONLYOFFICE@@core-v6.3.0.70-CVE-2023-50980-TP.c
Method	void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2679
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2680
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2681
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2682
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2683
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2023-50980-TP.c
Line	147	147

Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2684
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2685
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2686
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2687
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v7.2.0.130-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 16:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2688
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v7.2.0.130-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2689
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.3.0.5-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.3.0.5-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v7.3.0.5-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2690
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.3.0.5-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.3.0.5-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v7.3.0.5-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2691
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.3.3.6-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.3.3.6-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v7.3.3.6-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2692
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.3.3.6-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.3.3.6-CVE-2023-50980-TP.c
Line	153	153

Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v7.3.3.6-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2693
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.4.0.101-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.4.0.101-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v7.4.0.101-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2694
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.4.0.101-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.4.0.101-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v7.4.0.101-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2695
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.5.0.22-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.5.0.22-CVE-2023-50980-TP.c
Line	192	192
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v7.5.0.22-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
192.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2696
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.5.0.22-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.5.0.22-CVE-2023-50980-TP.c
Line	198	198
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v7.5.0.22-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
198.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 25:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2697
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.6.0.2-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.6.0.2-CVE-2023-50980-TP.c
Line	192	192
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v7.6.0.2-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
192.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2698
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.6.0.2-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v7.6.0.2-CVE-2023-50980-TP.c
Line	198	198
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v7.6.0.2-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
198.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2699
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v8.0.1.26-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v8.0.1.26-CVE-2023-50980-TP.c
Line	192	192
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v8.0.1.26-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
192.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2700
Status New

	Source	Destination
File	ONLYOFFICE@@core-v8.0.1.26-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v8.0.1.26-CVE-2023-50980-TP.c
Line	198	198
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v8.0.1.26-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
198.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2701
Status New

	Source	Destination
File	ONLYOFFICE@@core-v8.1.0.126-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v8.1.0.126-CVE-2023-50980-TP.c
Line	192	192

Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v8.1.0.126-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
192.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2702
Status New

	Source	Destination
File	ONLYOFFICE@@core-v8.1.0.126-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v8.1.0.126-CVE-2023-50980-TP.c
Line	198	198
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v8.1.0.126-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
198.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2703
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2704
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Uncontrolled Recursion\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2705
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2268-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v99.99.99.2268-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2268-CVE-2023-50980-TP.c
Method void PolynomialMod2::Decode(const byte *input, size_t inputLen)

```
....
147.        Decode(store, inputLen);
```

Uncontrolled Recursion\Path 34:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2706
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2268-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v99.99.99.2268-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2268-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Divide By Zero

Query Path:
CPP\Cx\CPP Medium Threat\Divide By Zero Version:1

Description

Divide By Zero\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1194
Status	New

The application performs an illegal operation in canon_a5_load_raw, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 548, the program attempts to divide by bc, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input bc in canon_a5_load_raw of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 548.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	566	566
Object	bc	bc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS canon_a5_load_raw()

```
....
566.    if (bc) black /= bc;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1195
Status	New

The application performs an illegal operation in canon_a5_load_raw, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 548, the program attempts to divide by bc, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input bc in canon_a5_load_raw of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 548.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	566	566
Object	bc	bc

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS canon_a5_load_raw()

```
....
566.    if (bc) black /= bc;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1196
Status	New

The application performs an illegal operation in main, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 8313, the program attempts to divide by pixel_aspect, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input pixel_aspect in main of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8559	8559
Object	pixel_aspect	pixel_aspect

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8559.           if (pixel_aspect < 1) iheight = iheight / pixel_aspect +
0.5;
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1197
Status	New

The application performs an illegal operation in remove_zeroes, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 520, the program attempts to divide by n, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input n in remove_zeroes of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 520.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	533	533
Object	n	n

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS remove_zeroes()

```
....
533.        if (n) BAYER(row,col) = tot/n;
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1198
Status	New

The application performs an illegal operation in main, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 8313, the program attempts to divide by pixel_aspect, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input pixel_aspect in main of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8559	8559
Object	pixel_aspect	pixel_aspect

Code Snippet	
File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	int CLASS main (int argc, char **argv)

```
....
8559.           if (pixel_aspect < 1) iheight = iheight / pixel_aspect +
0.5;
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1199
Status	New

The application performs an illegal operation in remove_zeroes, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 520, the program attempts to divide by n, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input n in remove_zeroes of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 520.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	533	533
Object	n	n

Code Snippet	
File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS remove_zeroes()

```
....
533.        if (n) BAYER(row,col) = tot/n;
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1200
Status	New

The application performs an illegal operation in cam_xyz_coeff, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 3545, the program attempts to divide by num, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num in cam_xyz_coeff of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 3545.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-	ONLYOFFICE@@core-v5.5.99.2024-CVE-

	2022-29776-FP.c	2022-29776-FP.c
Line	3559	3559
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS cam_xyz_coeff (double cam_xyz[4][3])

```
....
3559.         cam_rgb[i][j] /= num;
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1201
Status	New

The application performs an illegal operation in scale_colors, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 3748, the program attempts to divide by dmax, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input dmax in scale_colors of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 3748.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3812	3812
Object	dmax	dmax

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS scale_colors()

```
....
3812.     FORC4 scale_mul[c] = (pre_mul[c] /= dmax) * 65535.0 / maximum;
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1202
Status	New

The application performs an illegal operation in foveon_interpolate, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 3014, the program attempts to divide by num, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external,

untrusted input num in foveon_interpolate of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 3014.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3079	3079
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3079.     FORC3 div[c] /= num;
```

Divide By Zero\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1203
Status	New

The application performs an illegal operation in cam_xyz_coeff, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 3545, the program attempts to divide by num, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num in cam_xyz_coeff of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 3545.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3559	3559
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS cam_xyz_coeff (double cam_xyz[4][3])

```
....
3559.         cam_rgb[i][j] /= num;
```

Divide By Zero\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1204
Status	New

The application performs an illegal operation in scale_colors, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 3748, the program attempts to divide by dmax, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input dmax in scale_colors of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 3748.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3812	3812
Object	dmax	dmax

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS scale_colors()

```
....
3812.    FORC4 scale_mul[c] = (pre_mul[c] /= dmax) * 65535.0 / maximum;
```

Divide By Zero\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1205
Status New

The application performs an illegal operation in foveon_make_curve, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 2976, the program attempts to divide by max, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input max in foveon_make_curve of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 2976.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2989	2989
Object	max	max

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method short * CLASS foveon_make_curve (double max, double mul, double filt)

```
....
2989.      x = i*filt/max/4;
```

Divide By Zero\Path 13:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1206
Status	New

The application performs an illegal operation in bad_pixels, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 3417, the program attempts to divide by n, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input n in bad_pixels of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 3417.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3465	3465
Object	n	n

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3465.       BAYER2(row,col) = tot/n;
```

Divide By Zero\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1207
Status	New

The application performs an illegal operation in cam_xyz_coeff, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 3545, the program attempts to divide by num, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num in cam_xyz_coeff of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 3545.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3560	3560
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS cam_xyz_coeff (double cam_xyz[4][3])

```
....
3560.       pre_mul[i] = 1 / num;
```

Divide By Zero\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1208
Status	New

The application performs an illegal operation in scale_colors, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 3748, the program attempts to divide by maximum, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input maximum in scale_colors of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 3748.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3812	3812
Object	maximum	maximum

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS scale_colors()

```
....
3812.    FORC4 scale_mul[c] = (pre_mul[c] /= dmax) * 65535.0 / maximum;
```

Divide By Zero\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1209
Status	New

The application performs an illegal operation in vng_interpolate, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 3962, the program attempts to divide by num, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num in vng_interpolate of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 3962.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4073	4073
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4073.          t += (sum[c] - sum[color]) / num;
```

Divide By Zero\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1210
Status	New

The application performs an illegal operation in recover_highlights, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 4339, the program attempts to divide by wgt, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input wgt in recover_highlights of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 4339.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4373	4373
Object	wgt	wgt

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS recover_highlights()

```
....
4373.          map[mrow*wide+mcol] = sum / wgt;
```

Divide By Zero\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1211
Status	New

The application performs an illegal operation in gamma_lut, in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. In line 8111, the program attempts to divide by white, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input white in gamma_lut of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, at line 8111.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8126	8126
Object	white	white

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS gamma_lut (uchar lut[0x10000])

```
....
8126.       r = i / white;
```

Divide By Zero\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1212
Status	New

The application performs an illegal operation in foveon_make_curve, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 2976, the program attempts to divide by filt, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input filt in foveon_make_curve of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 2976.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2983	2983
Object	filt	filt

Code Snippet	
File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	short * CLASS foveon_make_curve (double max, double mul, double filt)

```
....
2983.     size = 4*M_PI*max / filt;
```

Divide By Zero\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1213
Status	New

The application performs an illegal operation in foveon_make_curve, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 2976, the program attempts to divide by max, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input max in foveon_make_curve of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 2976.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-	ONLYOFFICE@@core-v99.99.99.2148-

	CVE-2022-29776-FP.c	CVE-2022-29776-FP.c
Line	2989	2989
Object	max	max

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method short * CLASS foveon_make_curve (double max, double mul, double filt)

```
....
2989.       x = i*filt/max/4;
```

Divide By Zero\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1214
Status	New

The application performs an illegal operation in bad_pixels, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 3417, the program attempts to divide by n, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input n in bad_pixels of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 3417.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3465	3465
Object	n	n

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3465.       BAYER2(row,col) = tot/n;
```

Divide By Zero\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1215
Status	New

The application performs an illegal operation in cam_xyz_coeff, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 3545, the program attempts to divide by num, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num in cam_xyz_coeff of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 3545.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3560	3560
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS cam_xyz_coeff (double cam_xyz[4][3])

```
....
3560.       pre_mul[i] = 1 / num;
```

Divide By Zero\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1216
Status New

The application performs an illegal operation in scale_colors, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 3748, the program attempts to divide by maximum, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input maximum in scale_colors of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 3748.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3812	3812
Object	maximum	maximum

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS scale_colors()

```
....
3812.     FORC4 scale_mul[c] = (pre_mul[c] /= dmax) * 65535.0 / maximum;
```

Divide By Zero\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1217
Status New

The application performs an illegal operation in vng_interpolate, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 3962, the program attempts to divide by num, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num in vng_interpolate of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 3962.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4073	4073
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4073.          t += (sum[c] - sum[color]) / num;
```

Divide By Zero\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1218
Status New

The application performs an illegal operation in recover_highlights, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 4339, the program attempts to divide by wgt, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input wgt in recover_highlights of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 4339.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4373	4373
Object	wgt	wgt

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS recover_highlights()

```
....
4373.          map[mrow*wide+mcol] = sum / wgt;
```

Divide By Zero\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1219
Status	New

The application performs an illegal operation in gamma_lut, in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. In line 8111, the program attempts to divide by white, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input white in gamma_lut of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, at line 8111.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8126	8126
Object	white	white

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS gamma_lut (uchar lut[0x10000])

```
....
8126.       r = i / white;
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2073
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	628	642
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Method	uchar * CLASS make_decoder (const uchar *source, int level)

```
....
628.    struct decode *cur;
....
642.        cur->branch[0] = free_decode;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2074
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	628	633
Object	cur	cur

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	uchar * CLASS make_decoder (const uchar *source, int level)

```
....
628.    struct decode *cur;
....
633.    cur = free_decode++;
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2075
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	628	644
Object	cur	branch

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	uchar * CLASS make_decoder (const uchar *source, int level)

```
....
628.    struct decode *cur;
....
644.        cur->branch[1] = free_decode;
```

Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2076
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by leaf at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	628	647
Object	cur	leaf

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	uchar * CLASS make_decoder (const uchar *source, int level)

```
....
628.    struct decode *cur;
....
647.        cur->leaf = source[16 + leaf++];
```

Use of Uninitialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2077
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Line	2105	2109
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method const int * CLASS make_decoder_int (const int *source, int level)

```
....
2105.    struct decode *cur;
....
2109.      cur->branch[0] = free_decode;
```

Use of Uninitialized Pointer\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2078
Status New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2105	2107
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method const int * CLASS make_decoder_int (const int *source, int level)

```
....
2105.    struct decode *cur;
....
2107.    cur = free_decode++;
```

Use of Uninitialized Pointer\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2079
Status New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2105	2111
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method const int * CLASS make_decoder_int (const int *source, int level)

```
....
2105.    struct decode *cur;
....
2111.      cur->branch[1] = free_decode;
```

Use of Uninitialized Pointer\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2080
Status New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by leaf at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2105	2114
Object	cur	leaf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method const int * CLASS make_decoder_int (const int *source, int level)

```
....
2105.    struct decode *cur;
....
2114.      cur->leaf = source[1];
```

Use of Uninitialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2081
Status New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by leaf at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2775	2791
Object	cur	leaf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_decoder (unsigned size, unsigned code)

```
....
2775.    struct decode *cur;
....
2791.        cur->leaf = i;
```

Use of Uninitialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2082
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2775	2783
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_decoder (unsigned size, unsigned code)

```
....
2775.    struct decode *cur;
....
2783.    cur = free_decode++;
```

Use of Uninitialized Pointer\Path 11:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2083
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2775	2797
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_decoder (unsigned size, unsigned code)

```
....
2775.    struct decode *cur;
....
2797.    cur->branch[0] = free_decode;
```

Use of Uninitialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2084
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2775	2799
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_decoder (unsigned size, unsigned code)

```
....
2775.    struct decode *cur;
....
2799.    cur->branch[1] = free_decode;
```

Use of Uninitialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2085
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by branch at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	628	642
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method uchar * CLASS make_decoder (const uchar *source, int level)

```
....
628.    struct decode *cur;
....
642.        cur->branch[0] = free_decode;
```

Use of Uninitialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2086
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	628	633
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method uchar * CLASS make_decoder (const uchar *source, int level)

```
....
628.    struct decode *cur;
....
633.    cur = free_decode++;
```

Use of Uninitialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2087
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by branch at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	628	644
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method uchar * CLASS make_decoder (const uchar *source, int level)

```
....
628.    struct decode *cur;
....
644.        cur->branch[1] = free_decode;
```

Use of Uninitialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2088
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by leaf at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	628	647
Object	cur	leaf

Code Snippet	
File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	uchar * CLASS make_decoder (const uchar *source, int level)

```
....
628.    struct decode *cur;
....
647.        cur->leaf = source[16 + leaf++];
```

Use of Uninitialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2089
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by branch at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2105	2109
Object	cur	branch

Code Snippet	
File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	const int * CLASS make_decoder_int (const int *source, int level)

```
....
2105.    struct decode *cur;
....
2109.      cur->branch[0] = free_decode;
```

Use of Uninitialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2090
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-	ONLYOFFICE@@core-v99.99.99.2148-

	CVE-2022-29776-FP.c	CVE-2022-29776-FP.c
Line	2105	2107
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method const int * CLASS make_decoder_int (const int *source, int level)

```
....
2105.    struct decode *cur;
....
2107.    cur = free_decode++;
```

Use of Uninitialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2091
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by branch at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2105	2111
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method const int * CLASS make_decoder_int (const int *source, int level)

```
....
2105.    struct decode *cur;
....
2111.      cur->branch[1] = free_decode;
```

Use of Uninitialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2092
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by leaf at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2105	2114
Object	cur	leaf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method const int * CLASS make_decoder_int (const int *source, int level)

```
....
2105.    struct decode *cur;
....
2114.      cur->leaf = source[1];
```

Use of Uninitialized Pointer\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2093
Status New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by leaf at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2775	2791
Object	cur	leaf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_decoder (unsigned size, unsigned code)

```
....
2775.    struct decode *cur;
....
2791.       cur->leaf = i;
```

Use of Uninitialized Pointer\Path 22:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2094
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2775	2783
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_decoder (unsigned size, unsigned code)

```
....
2775.    struct decode *cur;
....
2783.    cur = free_decode++;
```

Use of Uninitialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2095
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by branch at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2775	2797
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_decoder (unsigned size, unsigned code)

```
....
2775.    struct decode *cur;
....
2797.    cur->branch[0] = free_decode;
```

Use of Uninitialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2096
Status	New

The variable declared in cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by cur at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2775	2799
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_decoder (unsigned size, unsigned code)

```
....
2775.    struct decode *cur;
....
2799.    cur->branch[1] = free_decode;
```

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=1020062&projectid=20045&pathid=636
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8066 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Line	8079	8079
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS stretch()

```
....
8079.         frac = rc - (c = rc);
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=637
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8066 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8091	8091
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS stretch()

```
....
8091.         frac = rc - (c = rc);
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=638
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8066 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Line	8079	8079
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS stretch()

```
....
8079.         frac = rc - (c = rc);
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=639
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8066 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8091	8091
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS stretch()

```
....
8091.         frac = rc - (c = rc);
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=640
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 413 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Line	419	419
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS canon_600_auto_wb()

```
....
419.    i = canon_ev + 0.5;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=641
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1479 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1595	1595
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS phase_one_correct()

```
....
1595.       i = ((mult[0] * (1-cfrac) + mult[1] * cfrac)
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=642
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1479 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Line	1586	1586
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS phase_one_correct()

```
....
1586.       cfrac -= cip = cfrac;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=643
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4339 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4375	4375
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS recover_highlights()

```
....
4375.       for (spread = 32/grow; spread--; ) {
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=644
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8111 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Line	8127	8127
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS gamma_lut (uchar lut[0x10000])

```
....
8127.      val = 256 * ( !use_gamma ? r :
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=645
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 413 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	419	419
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS canon_600_auto_wb()

```
....
419.    i = canon_ev + 0.5;
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=646
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1479 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Line	1595	1595
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS phase_one_correct()

```
....
1595.       i = ((mult[0] * (1-cfrac) + mult[1] * cfrac)
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=647
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1479 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	1586	1586
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS phase_one_correct()

```
....
1586.       cfrac -= cip = cfrac;
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=648
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4339 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Line	4375	4375
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS recover_highlights()

```
....
4375.       for (spread = 32/grow; spread--; ) {
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=649
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8111 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8127	8127
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS gamma_lut (uchar lut[0x10000])

```
....
8127.       val = 256 * ( !use_gamma ? r :
```

Float Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Float Overflow Version:1

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

Float Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=624

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3088	3088
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3088.       FORC3 last[i][c] = trans[i][c] * dsum / trsum[i];
```

Float Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=625
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3545 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3560	3560
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS cam_xyz_coeff (double cam_xyz[4][3])

```
....
3560.       pre_mul[i] = 1 / num;
```

Float Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=626
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3748 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3812	3812
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS scale_colors()

```
....
3812.    FORC4 scale_mul[c] = (pre_mul[c] /= dmax) * 65535.0 / maximum;
```

Float Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=627
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4913 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5111	5111
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5111.          FORC4 rgb_cam[i][c] /= num;
```

Float Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=628
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8028 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8048	8048
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS fuji_rotate()

```
....
8048.         ur = r = fuji_width + (row-col)*step;
```

Float Overflow\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=629
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8028 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8049	8049
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS fuji_rotate()

```
....
8049.         uc = c = (row+col)*step;
```

Float Overflow\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=630
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3014 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3088	3088
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3088.       FORC3 last[i][c] = trans[i][c] * dsum / trsum[i];
```

Float Overflow\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=631
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3545 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3560	3560
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS cam_xyz_coeff (double cam_xyz[4][3])

```
....
3560.       pre_mul[i] = 1 / num;
```

Float Overflow\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=632
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3748 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3812	3812
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS scale_colors()

```
....
3812.    FORC4 scale_mul[c] = (pre_mul[c] /= dmax) * 65535.0 / maximum;
```

Float Overflow\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=633
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4913 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5111	5111
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5111.          FORC4 rgb_cam[i][c] /= num;
```

Float Overflow\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=634
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8028 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8048	8048
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS fuji_rotate()

```
....
8048.         ur = r = fuji_width + (row-col)*step;
```

Float Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=635
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8028 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8049	8049
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS fuji_rotate()

```
....
8049.         uc = c = (row+col)*step;
```

Short Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Short Overflow Version:1

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

Short Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=650
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4913 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5203	5203
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5203.        order = i;
```

Short Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=651
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2183	2183
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2183.        buf[c][0][i] = (buf[c][0][i] * val + x) >> s;
```

Short Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=652
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2193	2193
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2193.              FORYX buf[c][y][x] = radc_token(tree+10) * 16 +
PREDICTOR;
```

Short Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=653
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2199	2199
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2199.              FORYX buf[c][y][x] = PREDICTOR;
```

Short Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=654
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2202	2202
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2202.                FORYX buf[c][y][x] += step;
```

Short Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=655
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4913 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5203	5203
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5203.        order = i;
```

Short Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=656
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2183	2183
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2183.       buf[c][0][i] = (buf[c][0][i] * val + x) >> s;
```

Short Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=657
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2193	2193
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2193.             FORYX buf[c][y][x] = radc_token(tree+10) * 16 +
PREDICTOR;
```

Short Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=658
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2199	2199
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2199.              FORYX buf[c][y][x] = PREDICTOR;
```

Short Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=659
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2202	2202
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2202.                FORYX buf[c][y][x] += step;
```

MemoryFree on StackVariable

Query Path:

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1264
Status	New

Calling free() (line 3014) on a variable that was not dynamically allocated (line 3014) in file ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3210	3210
Object	badpix	badpix

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3210.       free (badpix);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1265
Status	New

Calling free() (line 3014) on a variable that was not dynamically allocated (line 3014) in file ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3394	3394
Object	shrink	shrink

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3394.     free (shrink);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1266
Status	New

Calling free() (line 4913) on a variable that was not dynamically allocated (line 4913) in file ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5189	5189
Object	cbuf	cbuf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5189.       free (cbuf);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1267
Status	New

Calling free() (line 4913) on a variable that was not dynamically allocated (line 4913) in file ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5302	5302
Object	buf	buf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5302.       free (buf);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1268
Status	New

Calling free() (line 3014) on a variable that was not dynamically allocated (line 3014) in file ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3394	3394
Object	shrink	shrink

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3394.    free (shrink);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1269
Status	New

Calling free() (line 4913) on a variable that was not dynamically allocated (line 4913) in file ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5189	5189
Object	cbuf	cbuf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5189.        free (cbuf);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1270
Status	New

Calling free() (line 4913) on a variable that was not dynamically allocated (line 4913) in file ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5302	5302
Object	buf	buf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5302.       free (buf);
```

Stored Buffer Overflow cpycat

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow cpycat Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description
Stored Buffer Overflow cpycat\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2185
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Stored Buffer Overflow cpycat\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2186
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS parse_mos (int offset)

```
....
4851.        fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Stored Buffer Overflow cpycat\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2187
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Stored Buffer Overflow cpycat\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2188
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
....
4833.        strcpy (model, mod[i]);
```

Stored Buffer Overflow cpycat\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2189
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.       fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Stored Buffer Overflow cpycat\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2190
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_mos passes to Address, at line 4805 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.        fscanf (ifp, "%d", &i);
....
4833.       strcpy (model, mod[i]);
```

Memory Leak

Query Path:
CPP\Cx\CPP Medium Threat\Memory Leak Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Memory Leak\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2068
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	870	870
Object	row	row

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS ljpeg_start (struct jhead *jh, int info_only)

```
....
870.    jh->row = (ushort *) calloc (jh->wide*jh->clrs, 4);
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2069
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2985	2985
Object	curve	curve

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method short * CLASS foveon_make_curve (double max, double mul, double filt)

```
....
2985.    curve = (short *) calloc (size+1, sizeof *curve);
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2070

Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2985	2985
Object	curve	curve

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method short * CLASS foveon_make_curve (double max, double mul, double filt)

```
....
2985.    curve = (short *) calloc (size+1, sizeof *curve);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2071
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2937	2937
Object	size	size

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void * CLASS foveon_camf_matrix (unsigned dim[3], const char *name)

```
....
2937.      mat = (unsigned *) malloc ((size = dsize) * 4);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2072
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c

Line	2937	2937
Object	size	size

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void * CLASS foveon_camf_matrix (unsigned dim[3], const char *name)

```
....
2937.      mat = (unsigned *) malloc ((size = dsize) * 4);
```

Buffer Overflow AddressOfLocalVarReturned

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=375
Status	New

The pointer sum at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 6521 is being used after it has been freed.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	6537	6537
Object	sum	sum

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method short CLASS guess_byte_order (int words)

```
....
6537.    return sum[0] < sum[1] ? 0x4d4d : 0x4949;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=376

Status	New

The pointer sum at ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c in line 6521 is being used after it has been freed.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	6537	6537
Object	sum	sum

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method short CLASS guess_byte_order (int words)

```
....
6537.    return sum[0] < sum[1] ? 0x4d4d : 0x4949;
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=377
Status	New

The pointer sum at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 6521 is being used after it has been freed.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	6537	6537
Object	sum	sum

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method short CLASS guess_byte_order (int words)

```
....
6537.    return sum[0] < sum[1] ? 0x4d4d : 0x4949;
```

Buffer Overflow AddressOfLocalVarReturned\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=378
Status	New

The pointer sum at ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c in line 6521 is being used after it has been freed.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	6537	6537
Object	sum	sum

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method short CLASS guess_byte_order (int words)

```
....
6537.    return sum[0] < sum[1] ? 0x4d4d : 0x4949;
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Variable\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2097
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3676	3717
Object	lpass	lpass

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS wavelet_denoise()

```
....
3676.    int scale=1, size, lev, hpass, lpass, row, col, nc, c, i,
wlast;
....
3717.        image[i][c] = CLIP(SQR(fimg[i]+fimg[lpass+i])/0x10000);
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2098
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3676	3717
Object	lpass	lpass

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS wavelet_denoise()

```
....
3676.    int scale=1, size, lev, hpass, lpass, row, col, nc, c, i,
wlast;
....
3717.        image[i][c] = CLIP(SQR(fimg[i]+fimg[lpass+i])/0x10000);
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2099
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3676	3717
Object	lpass	lpass

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS wavelet_denoise()

```
....
3676.    int scale=1, size, lev, hpass, lpass, row, col, nc, c, i,
wlast;
....
3717.        image[i][c] = CLIP(SQR(fimg[i]+fimg[lpass+i])/0x10000);
```

Use of Uninitialized Variable\Path 4:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2100
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3676	3717
Object	lpass	lpass

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS wavelet_denoise()

```
....
3676.    int scale=1, size, lev, hpass, lpass, row, col, nc, c, i,
wlast;
....
3717.        image[i][c] = CLIP(SQR(fimg[i]+fimg[lpass+i])/0x10000);
```

Off by One Error in Loops

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description
Off by One Error in Loops\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=618
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 972 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	983	983
Object	<=	<=

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method	void CLASS canon_sraw_load_raw()

```
....
983.    for (ecol=slice=0; slice <= cr2_slice[0]; slice++) {
```

Off by One Error in Loops\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=619
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 972 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	983	983
Object	<=	<=

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS canon_sraw_load_raw()

```
....
983.    for (ecol=slice=0; slice <= cr2_slice[0]; slice++) {
```

Wrong Size t Allocation

Query Path:
CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0

Description

Wrong Size t Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=620
Status	New

The function dsize in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 2916 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2937	2937

Object	dsize	dsize

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void * CLASS foveon_camf_matrix (unsigned dim[3], const char *name)

```
....
2937.      mat = (unsigned *) malloc ((size = dsize) * 4);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=621
Status	New

The function dsize in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 2916 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2937	2937
Object	dsize	dsize

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void * CLASS foveon_camf_matrix (unsigned dim[3], const char *name)

```
....
2937.      mat = (unsigned *) malloc ((size = dsize) * 4);
```

Char Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Char Overflow Version:1

Categories

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

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=622
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2049 of OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2130	2130
Object	AssignExpr	AssignExpr

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsassa_pss_verify_ext(mbedtls_rsa_context *ctx,

```
....
2130.      buf[0] &= 0xFF >> (siglen * 8 - msb);
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=623
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2049 of OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c
Line	2130	2130
Object	AssignExpr	AssignExpr

Code Snippet
File Name OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsassa_pss_verify_ext(mbedtls_rsa_context *ctx,

```
....
2130.      buf[0] &= 0xFF >> (siglen * 8 - msb);
```

Double Free

Query Path:
CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description

Double Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2066
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3448	3448
Object	fname	fname

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3448.       free (fname);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2067
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3448	3448
Object	fname	fname

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3448.       free (fname);
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1271
Status	New

The variable declared in null at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 242 is not initialized when it is used by dev at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 242.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	245	301
Object	null	dev

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
245.      ogs_pfcp_subnet_t *subnet = NULL;
....
301.          ogs_assert(subnet->dev);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1272
Status	New

The variable declared in null at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 242 is not initialized when it is used by dev at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 242.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	245	304
Object	null	dev

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method int upf_gtp_open(void)

```
....
245.      ogs_pfcp_subnet_t *subnet = NULL;
....
304.              ogs_error("ogs_tun_set_ip(dev:%s) failed", subnet-
>dev->ifname);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1273
Status	New

The variable declared in null at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316 is not initialized when it is used by fd at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	318	325
Object	null	fd

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
318.      ogs_pfcp_dev_t *dev = NULL;
....
325.          ogs_closesocket(dev->fd);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1274
Status	New

The variable declared in null at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316 is not initialized when it is used by poll at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	318	324
Object	null	poll

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
318.      ogs_pfcp_dev_t *dev = NULL;
....
324.              ogs_pollset_remove(dev->poll);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1275
Status	New

The variable declared in null at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316 is not initialized when it is used by poll at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 316.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	318	323
Object	null	poll

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method void upf_gtp_close(void)

```
....
318.      ogs_pfcp_dev_t *dev = NULL;
....
323.          if (dev->poll)
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1276
Status	New

The variable declared in null at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 428 is not initialized when it is used by ipv6 at open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c in line 428.

	Source	Destination
File	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c	open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Line	445	449

Object	null	ipv6

Code Snippet
File Name open5gs@@open5gs-v1.3.0-CVE-2021-45462-FP.c
Method static int upf_gtp_handle_multicast(ogs_pkbuf_t *recvbuf)

```
....
445.              upf_sess_t *sess = NULL;
....
449.                  if (sess->ipv6) {
```

NULL Pointer Dereference\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1277
Status New

The variable declared in null at open5gs@@open5gs-v2.2.0-CVE-2023-50019-FP.c in line 90 is not initialized when it is used by paging at open5gs@@open5gs-v2.2.0-CVE-2023-50019-FP.c in line 90.

	Source	Destination
File	open5gs@@open5gs-v2.2.0-CVE-2023-50019-FP.c	open5gs@@open5gs-v2.2.0-CVE-2023-50019-FP.c
Line	340	346
Object	null	paging

Code Snippet
File Name open5gs@@open5gs-v2.2.0-CVE-2023-50019-FP.c
Method static void common_register_state(ogs_fsm_t *s, amf_event_t *e)

```
....
340.                  amf_sess_t *sess = NULL;
....
346.                      if (sess->paging.ongoing == true) {
```

NULL Pointer Dereference\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1278
Status New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2439 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-	OP-TEE@@optee_os-4.0.0-rc1-CVE-

	2024-23170-TP.c	2024-23170-TP.c
Line	2543	1997
Object	null	len

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2543.       if (mbedtls_rsa_pkcs1_sign(&rsa, myrand, NULL,
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
1997.       memcpy(sig, sig_try, ctx->len);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1279
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 75 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	94	1997
Object	0	len

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
94.       return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
1997.       memcpy(sig, sig_try, ctx->len);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1280
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 141 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	222	1997
Object	0	len

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
222.       return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
1997.       memcpy(sig, sig_try, ctx->len);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1281
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2439 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Line	2543	2000
Object	null	len

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2543.       if (mbedtls_rsa_pkcs1_sign(&rsa, myrand, NULL,
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
2000.       mbedtls_platform_zeroize(sig_try, ctx->len);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1282
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 75 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	94	2000
Object	0	len

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
94.       return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
2000.       mbedtls_platform_zeroize(sig_try, ctx->len);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1283
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 141 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	222	2000
Object	0	len

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
222.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
2000.      mbedtls_platform_zeroize(sig_try, ctx->len);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1284
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2439 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2543	2001
Object	null	len

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2543.       if (mbedtls_rsa_pkcs1_sign(&rsa, myrand, NULL,
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
2001.       mbedtls_platform_zeroize(verif, ctx->len);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1285
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 75 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	94	2001
Object	0	len

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
94.       return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
2001.       mbedtls_platform_zeroize(verif, ctx->len);
```

NULL Pointer Dereference\Path 16:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1286
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 141 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	222	2001
Object	0	len

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
222.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
2001.      mbedtls_platform_zeroize(verif, ctx->len);
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1287
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 75 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	94	2006
Object	0	len

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
94.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
2006.          memset(sig, '!', ctx->len);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1288
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 141 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	222	2006
Object	0	len

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
222.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
2006.          memset(sig, '!', ctx->len);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1289
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2439 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1944.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2543	2006
Object	null	len

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2543.      if (mbedtls_rsa_pkcs1_sign(&rsa, myrand, NULL,
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsassa_pkcs1_v15_sign(mbedtls_rsa_context *ctx,

```
....
2006.          memset(sig, '!', ctx->len);
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1290
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 75 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 726.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	94	746
Object	0	len

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
94.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_public(mbedtls_rsa_context *ctx,

```
....
746.      MBEDTLS_MPI_CHK(mbedtls_mpi_read_binary(&T, input, ctx->len));
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1291
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 141 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 726.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	222	746
Object	0	len

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
222.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_public(mbedtls_rsa_context *ctx,

```
....
746.      MBEDTLS_MPI_CHK(mbedtls_mpi_read_binary(&T, input, ctx->len));
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1292
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2439 is not initialized when it is used by len at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 726.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2543	746
Object	null	len

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2543.      if (mbedtls_rsa_pkcs1_sign(&rsa, myrand, NULL,
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_public(mbedtls_rsa_context *ctx,

```
....
746.      MBEDTLS_MPI_CHK(mbedtls_mpi_read_binary(&T, input, ctx->len));
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1293
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 75 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 726.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	94	754
Object	0	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
94.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_public(mbedtls_rsa_context *ctx,

```
....
754.      MBEDTLS_MPI_CHK(mbedtls_mpi_exp_mod(&T, &T, &ctx->E, &ctx->N,
&ctx->RN));
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1294
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 141 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 726.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	222	754
Object	0	N

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
222.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_public(mbedtls_rsa_context *ctx,

```
....
754.      MBEDTLS_MPI_CHK(mbedtls_mpi_exp_mod(&T, &T, &ctx->E, &ctx->N,
&ctx->RN));
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1295
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2439 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 726.

	Source	Destination

File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2543	754
Object	null	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2543.      if (mbedtls_rsa_pkcs1_sign(&rsa, myrand, NULL,
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_public(mbedtls_rsa_context *ctx,

```
....
754.      MBEDTLS_MPI_CHK(mbedtls_mpi_exp_mod(&T, &T, &ctx->E, &ctx->N,
&ctx->RN));
```

NULL Pointer Dereference\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1296
Status New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 75 is not initialized when it is used by E at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 726.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	94	754
Object	0	E

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
94.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_public(mbedtls_rsa_context *ctx,

```
....
754.      MBEDTLS_MPI_CHK(mbedtls_mpi_exp_mod(&T, &T, &ctx->E, &ctx->N,
&ctx->RN));
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1297
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 141 is not initialized when it is used by E at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 726.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	222	754
Object	0	E

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
222.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_public(mbedtls_rsa_context *ctx,

```
....
754.      MBEDTLS_MPI_CHK(mbedtls_mpi_exp_mod(&T, &T, &ctx->E, &ctx->N,
&ctx->RN));
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1298
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2439 is not initialized when it is used by E at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 726.

	Source	Destination

File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2543	754
Object	null	E

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2543.      if (mbedtls_rsa_pkcs1_sign(&rsa, myrand, NULL,
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_public(mbedtls_rsa_context *ctx,

```
....
754.      MBEDTLS_MPI_CHK(mbedtls_mpi_exp_mod(&T, &T, &ctx->E, &ctx->N,
&ctx->RN));
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1299
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1656 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1765	1033
Object	null	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method static int rsa_rsassa_pss_sign(mbedtls_rsa_context *ctx,

```
....
1765.          return mbedtls_rsa_private(ctx, NULL, NULL, sig, sig);
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                                   &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1300
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1456 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1499	1033
Object	null	N

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsaes_oaep_decrypt(mbedtls_rsa_context *ctx,

```
....
1499.          ret = mbedtls_rsa_private( ctx, NULL, NULL, input, buf );
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                                   &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1301
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1456 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Line	1499	1033
Object	null	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsaes_oaep_decrypt(mbedtls_rsa_context *ctx,

```
....
1499.           ret = mbedtls_rsa_private( ctx, NULL, NULL, input, buf );
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                           &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1302
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1656 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1765	1033
Object	null	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method static int rsa_rsassa_pss_sign(mbedtls_rsa_context *ctx,

```
....
1765.           return mbedtls_rsa_private(ctx, NULL, NULL, sig, sig);
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                           &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1303
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 75 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	94	1033
Object	0	N

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
94.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                          &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1304
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 141 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	222	1033
Object	0	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
222.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                          &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1305
Status New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2439 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2543	1033
Object	null	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2543.      if (mbedtls_rsa_pkcs1_sign(&rsa, myrand, NULL,
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                          &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 36:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1306
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1656 is not initialized when it is used by RN at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1765	1033
Object	null	RN

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method static int rsa_rsassa_pss_sign(mbedtls_rsa_context *ctx,

```
....
1765.          return mbedtls_rsa_private(ctx, NULL, NULL, sig, sig);
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                          &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1307
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1456 is not initialized when it is used by RN at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1499	1033
Object	null	RN

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsaes_oaep_decrypt(mbedtls_rsa_context *ctx,

```
....
1499.          ret = mbedtls_rsa_private( ctx, NULL, NULL, input, buf );
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                          &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1308
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1656 is not initialized when it is used by RN at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1765	1033
Object	null	RN

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method static int rsa_rsassa_pss_sign(mbedtls_rsa_context *ctx,

```
....
1765.          return mbedtls_rsa_private(ctx, NULL, NULL, sig, sig);
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                          &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1309
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1456 is not initialized when it is used by RN at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1499	1033
Object	null	RN

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsaes_oaep_decrypt(mbedtls_rsa_context *ctx,

```
....
1499.          ret = mbedtls_rsa_private( ctx, NULL, NULL, input, buf );
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                                 &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1310
Status New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 75 is not initialized when it is used by RN at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	94	1033
Object	0	RN

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
94.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                                   &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1311
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 141 is not initialized when it is used by RN at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	222	1033
Object	0	RN

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
222.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                                   &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1312
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2439 is not initialized when it is used by RN at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2543	1033
Object	null	RN

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2543.       if (mbedtls_rsa_pkcs1_sign(&rsa, myrand, NULL,
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1033.                                               &ctx->N, &ctx->RN));
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1313
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1656 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1765	1029
Object	null	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method static int rsa_rsassa_pss_sign(mbedtls_rsa_context *ctx,

```
....
1765.           return mbedtls_rsa_private(ctx, NULL, NULL, sig, sig);
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1029.       MBEDTLS_MPI_CHK(mbedtls_mpi_mod_mpi(&T, &T, &ctx->N));
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1314
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1456 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1499	1029
Object	null	N

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsaes_oaep_decrypt(mbedtls_rsa_context *ctx,

```
....
1499.           ret = mbedtls_rsa_private( ctx, NULL, NULL, input, buf );
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1029.       MBEDTLS_MPI_CHK(mbedtls_mpi_mod_mpi(&T, &T, &ctx->N));
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1315
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1656 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Line	1765	1029
Object	null	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method static int rsa_rsassa_pss_sign(mbedtls_rsa_context *ctx,

```
....
1765.          return mbedtls_rsa_private(ctx, NULL, NULL, sig, sig);
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1029.      MBEDTLS_MPI_CHK(mbedtls_mpi_mod_mpi(&T, &T, &ctx->N));
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1316
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1456 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1499	1029
Object	null	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_rsaes_oaep_decrypt(mbedtls_rsa_context *ctx,

```
....
1499.          ret = mbedtls_rsa_private( ctx, NULL, NULL, input, buf );
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1029.      MBEDTLS_MPI_CHK(mbedtls_mpi_mod_mpi(&T, &T, &ctx->N));
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1317
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 75 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	94	1029
Object	0	N

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_import(mbedtls_rsa_context *ctx,

```
....
94.       return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1029.       MBEDTLS_MPI_CHK(mbedtls_mpi_mod_mpi(&T, &T, &ctx->N));
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1318
Status	New

The variable declared in 0 at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 141 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	222	1029
Object	0	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method static int rsa_check_context(mbedtls_rsa_context const *ctx, int is_priv,

```
....
222.      return 0;
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1029.      MBEDTLS_MPI_CHK(mbedtls_mpi_mod_mpi(&T, &T, &ctx->N));
```

NULL Pointer Dereference\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1319
Status New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 2439 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2543	1029
Object	null	N

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method int mbedtls_rsa_self_test(int verbose)

```
....
2543.      if (mbedtls_rsa_pkcs1_sign(&rsa, myrand, NULL,
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
1029.      MBEDTLS_MPI_CHK(mbedtls_mpi_mod_mpi(&T, &T, &ctx->N));
```

NULL Pointer Dereference\Path 50:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1320
Status	New

The variable declared in null at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 1456 is not initialized when it is used by N at OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c in line 861.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	1499	998
Object	null	N

Code Snippet

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_rsaes_oaep_decrypt(mbedtls_rsa_context *ctx,

```
....
1499.          ret = mbedtls_rsa_private( ctx, NULL, NULL, input, buf );
```

File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c

Method int mbedtls_rsa_private(mbedtls_rsa_context *ctx,

```
....
998.       MBEDTLS_MPI_CHK(mbedtls_mpi_exp_mod(&T, &T, D, &ctx->N, &ctx->RN));
```

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=1020062&projectid=20045&pathid=2191
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3451	3451

Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3451.    while (fgets (line, 128, fp)) {
```

Improper Resource Access Authorization\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2192
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4546	4546
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_makernote (int base, int uptag)

```
....
4546.        fgets (model2, 64, ifp);
```

Improper Resource Access Authorization\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2193
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4785	4785
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_gps (int base)

```
....
4785.       fgets ((char *) (gpsdata+14+tag/3), MIN(len,12), ifp);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2194
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4977	4977
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4977.       fgets (make, 64, ifp);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2195
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4980	4980
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4980.       fgets (model, 64, ifp);
```

Improper Resource Access Authorization\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2196
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5011	5011
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5011.       fgets (software, 64, ifp);
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2197
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5076	5076
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5076.       fgets (model2, 64, ifp);
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2198
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5667	5667
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_rollei()

```
....
5667.      fgets (line, 128, ifp);
```

Improper Resource Access Authorization\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2199
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3451	3451
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3451.    while (fgets (line, 128, fp)) {
```

Improper Resource Access Authorization\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2200
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4546	4546

Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_makernote (int base, int uptag)

```
....
4546.         fgets (model2, 64, ifp);
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2201
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4785	4785
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_gps (int base)

```
....
4785.       fgets ((char *) (gpsdata+14+tag/3), MIN(len,12), ifp);
```

Improper Resource Access Authorization\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2202
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4977	4977
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4977.       fgets (make, 64, ifp);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2203
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4980	4980
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4980.       fgets (model, 64, ifp);
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2204
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5011	5011
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5011.       fgets (software, 64, ifp);
```

Improper Resource Access Authorization\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2205
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5076	5076
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5076.       fgets (model2, 64, ifp);
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2206
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5667	5667
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_rollei()

```
....
5667.      fgets (line, 128, ifp);
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2207
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4831	4831
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         fscanf (ifp, "%d", &i);
```

Improper Resource Access Authorization\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2208
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4842	4842
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.         fscanf (ifp, "%f", &romm_cam[0][i]);
```

Improper Resource Access Authorization\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2209
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4846	4846

Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4846.        fscanf (ifp, "%d", &planes);
```

Improper Resource Access Authorization\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2210
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4848	4848
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4848.        fscanf (ifp, "%d", &flip);
```

Improper Resource Access Authorization\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2211
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4851	4851
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.       fscanf (ifp, "%d", &i);
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2212
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4855	4855
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.       fscanf (ifp, "%d", &i);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2213
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4859	4859
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4859.       FORC4 fscanf (ifp, "%d", neut+c);
```

Improper Resource Access Authorization\Path 24:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2214
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5107	5107
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5107.          FORC4 fscanf (ifp, "%f", &rgb_cam[i][c^1]);
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2215
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4831	4831
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.          fscanf (ifp, "%d", &i);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2216
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4842	4842
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4842.       fscanf (ifp, "%f", &romm_cam[0][i]);
```

Improper Resource Access Authorization\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2217
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4846	4846
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4846.        fscanf (ifp, "%d", &planes);
```

Improper Resource Access Authorization\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2218
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4848	4848

Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4848.        fscanf (ifp, "%d", &flip);
```

Improper Resource Access Authorization\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2219
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4851	4851
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.        fscanf (ifp, "%d", &i);
```

Improper Resource Access Authorization\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2220
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4855	4855
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.        fscanf (ifp, "%d", &i);
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2221
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4859	4859
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4859.        FORC4 fscanf (ifp, "%d", neut+c);
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2222
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5107	5107
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5107.         FORC4 fscanf (ifp, "%f", &rgb_cam[i][c^1]);
```

Improper Resource Access Authorization\Path 33:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2223
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	336	336
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method double CLASS getreal (int type)

```
....
336.        u.c[i ^ rev] = fgetc(ifp);
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2224
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	338	338
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method double CLASS getreal (int type)

```
....
338.      default: return fgetc(ifp);
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2225
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	585	585
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
585.      if ((c = fgetc(ifp)) == EOF) derror();
```

Improper Resource Access Authorization\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2226
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	586	586
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

```
....
586.      if ((reset = zero_after_ff && c == 0xff && fgetc(ifp))) return
0;
```

Improper Resource Access Authorization\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2227
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	788	788

Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS canon_compressed_load_raw()

```
....
788.        c = fgetc(ifp);
```

Improper Resource Access Authorization\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2228
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	898	898
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method ushort * CLASS ljpeg_row (int jrow, struct jhead *jh)

```
....
898.        do mark = (mark << 8) + (c = fgetc(ifp));
```

Improper Resource Access Authorization\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2229
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1121	1121
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS pentax_tree()

```
....
1121.    FORC(13) bit[1][c] = fgetc(ifp) & 15;
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2230
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1170	1170
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS nikon_compressed_load_raw()

```
....
1170.    ver0 = fgetc(ifp);
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2231
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1171	1171
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS nikon_compressed_load_raw()

```
....
1171.    ver1 = fgetc(ifp);
```

Improper Resource Access Authorization\Path 42:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2232
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1246	1246
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS nikon_e995()

```
....
1246.       histo[fgetc(ifp)]++;
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2233
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2416	2416
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2416.       c = fgetc(ifp);
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2234
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2431	2431
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2431.       bitbuf  = fgetc(ifp) << 8;
```

Improper Resource Access Authorization\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2235
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2432	2432
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2432.       bitbuf += fgetc(ifp);
```

Improper Resource Access Authorization\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2236
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2439	2439

Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2439.       bitbuf += (INT64) fgetc(ifp) << (bits+(j^8));
```

Improper Resource Access Authorization\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2237
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2545	2545
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS sony_load_raw()

```
....
2545.    fseek (ifp, (unsigned) fgetc(ifp)*4 - 1, SEEK_CUR);
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2238
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2756	2756
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS smal_v9_load_raw()

```
....
2756.    nseg = fgetc(ifp);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2239
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2761	2761
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS smal_v9_load_raw()

```
....
2761.    holes = fgetc(ifp);
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2240
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2833	2833
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_thumb (FILE *tfp)

```
....
2833.            bitbuf = (bitbuf << 8) + fgetc(ifp);
```

Unchecked Array Index

Query Path:

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unchecked Array Index\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3000
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2023-50980-TP.c
Line	391	391
Object	carryIndex	carryIndex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2023-50980-TP.c
Method PolynomialMod2& PolynomialMod2::operator<<=(unsigned int n)

```
....
391.                reg[carryIndex] = carry;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3001
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1697	1697
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1697.                rarray[octindex] += rval;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3002
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1698	1698
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1698.              garray[octindex] += gval;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3003
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1699	1699
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1699.              barray[octindex] += bval;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3004
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1790	1790
Object	index	index

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1790.       iarray[opop->index] = i + 1;  /* +1 to avoid storing 0 */
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3005
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1821	1821
Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1821.           narray[octindex2] += (l_int32)opop->npix;
```

Unchecked Array Index\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3006
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1822	1822

Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1822.          rarray[octindex2] += (l_int32)opop->npix * rval;
```

Unchecked Array Index\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3007
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1823	1823
Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1823.          garray[octindex2] += (l_int32)opop->npix * gval;
```

Unchecked Array Index\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3008
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1824	1824
Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1824.          barray[octindex2] += (l_int32)opop->npix * bval;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3009
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1825	1825
Object	index	index

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1825.       iarray[opop->index] = 192 + octindex2 + 1;  /* +1 to avoid
storing 0 */
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3010
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	2400	2400
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2400.          lut1[oqca[nbase + i]->octindex] = nbase + i;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3011
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	2639	2639
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctcubeQuantMixedWithGray(PIX *pixs,

```
....
2639.                    rarray[octindex] += rval;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3012
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	2640	2640
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctcubeQuantMixedWithGray(PIX *pixs,

```
....
2640.                    garray[octindex] += gval;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3013
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	2641	2641
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctcubeQuantMixedWithGray(PIX *pixs,

```
....
2641.                    barray[octindex] += bval;
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3014
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	2917	2917
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixFewColorsOctcubeQuant1(PIX *pixs,

```
....
2917.                rarray[octindex] += rval;
```

Unchecked Array Index\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3015
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	2918	2918

Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixFewColorsOctcubeQuant1(PIX *pixs,

```
....
2918.              garray[octindex] += gval;
```

Unchecked Array Index\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3016
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	2919	2919
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixFewColorsOctcubeQuant1(PIX *pixs,

```
....
2919.              barray[octindex] += bval;
```

Unchecked Array Index\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3017
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	3121	3121
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixFewColorsOctcubeQuant2(PIX *pixs,

```
....
3121.                   octarray[octindex] = cindex;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3018
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	3122	3122
Object	cindex	cindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixFewColorsOctcubeQuant2(PIX *pixs,

```
....
3122.                   colorarray[cindex] = *ppixel;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3019
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	3691	3691
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctcubeHistogram(PIX *pixs,

```
....
3691.                 array[octindex] += 1.0;
```

Unchecked Array Index\Path 21:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3020
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2393	2393
Object	pi	pi

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_262_load_raw()

```
....
2393.         pixel[pi] = val = pred + ljpeg_diff (decode[chess]);
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3021
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3870	3870
Object	c	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS pre_interpolate()

```
....
3870.         img[row*width+col][c] = image[(row >> 1)*iwidth+(col >>
1)][c];
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3022
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3932	3932
Object	color	color

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS lin_interpolate()

```
....
3932.          sum[color] += 1 << shift;
```

Unchecked Array Index\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3023
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4121	4121
Object	c	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ppg_interpolate()

```
....
4121.        pix[0][c] = CLIP((pix[-d][c] + pix[d][c] + 2*pix[0][1]
```

Unchecked Array Index\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3024
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4136	4136

Object	c	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ppg_interpolate()

```
....
4136.       pix[0][c] = CLIP(guess[diff[0] > diff[1]] >> 1);
```

Unchecked Array Index\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3025
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4138	4138
Object	c	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ppg_interpolate()

```
....
4138.       pix[0][c] = CLIP((guess[0]+guess[1]) >> 2);
```

Unchecked Array Index\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3026
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4726	4726
Object	i	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS get_timestamp (int reversed)

```
....
4726.       for (i=19; i--; ) str[i] = fgetc(ifp);
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3027
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2023-50980-TP.c
Line	391	391
Object	carryIndex	carryIndex

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2023-50980-TP.c
Method PolynomialMod2& PolynomialMod2::operator<<=(unsigned int n)

```
....
391.                reg[carryIndex] = carry;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3028
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1697	1697
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX   *pixs,

```
....
1697.                rarray[octindex] += rval;
```

Unchecked Array Index\Path 30:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3029
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1698	1698
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1698.              garray[octindex] += gval;
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3030
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1699	1699
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1699.              barray[octindex] += bval;
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3031
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1790	1790
Object	index	index

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1790.       iarray[opop->index] = i + 1;  /* +1 to avoid storing 0 */
```

Unchecked Array Index\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3032
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1821	1821
Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1821.           narray[octindex2] += (l_int32)opop->npix;
```

Unchecked Array Index\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3033
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1822	1822

Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1822.          rarray[octindex2] += (l_int32)opop->npix * rval;
```

Unchecked Array Index\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3034
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1823	1823
Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1823.          garray[octindex2] += (l_int32)opop->npix * gval;
```

Unchecked Array Index\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3035
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1824	1824
Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1824.          barray[octindex2] += (l_int32)opop->npix * bval;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3036
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1825	1825
Object	index	index

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1825.       iarray[opop->index] = 192 + octindex2 + 1;  /* +1 to avoid
storing 0 */
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3037
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	2400	2400
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2400.          lut1[oqca[nbase + i]->octindex] = nbase + i;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3038
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	2639	2639
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctcubeQuantMixedWithGray(PIX *pixs,

```
....
2639.                    rarray[octindex] += rval;
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3039
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	2640	2640
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctcubeQuantMixedWithGray(PIX *pixs,

```
....
2640.                    garray[octindex] += gval;
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3040
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	2641	2641
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctcubeQuantMixedWithGray(PIX *pixs,

```
....
2641.                    barray[octindex] += bval;
```

Unchecked Array Index\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3041
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	2917	2917
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixFewColorsOctcubeQuant1(PIX *pixs,

```
....
2917.                rarray[octindex] += rval;
```

Unchecked Array Index\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3042
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	2918	2918

Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixFewColorsOctcubeQuant1(PIX *pixs,

```
....
2918.              garray[octindex] += gval;
```

Unchecked Array Index\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3043
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	2919	2919
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixFewColorsOctcubeQuant1(PIX *pixs,

```
....
2919.              barray[octindex] += bval;
```

Unchecked Array Index\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3044
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	3121	3121
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixFewColorsOctcubeQuant2(PIX *pixs,

```
....
3121.                   octarray[octindex] = cindex;
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3045
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	3122	3122
Object	cindex	cindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixFewColorsOctcubeQuant2(PIX *pixs,

```
....
3122.                   colorarray[cindex] = *ppixel;
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3046
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	3691	3691
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctcubeHistogram(PIX *pixs,

```
....
3691.                 array[octindex] += 1.0;
```

Unchecked Array Index\Path 48:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3047
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2023-50980-TP.c
Line	391	391
Object	carryIndex	carryIndex

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2023-50980-TP.c
Method PolynomialMod2& PolynomialMod2::operator<<=(unsigned int n)

```
....
391.              reg[carryIndex] = carry;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3048
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1697	1697
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1697.              rarray[octindex] += rval;
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=3049
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1698	1698
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1698.              garray[octindex] += gval;
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2872
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Line	301	301
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Method ccbaCreate(PIX *pixs,

```
....
301.      if ((ccba->ccb = (CCBORD **)CALLOC(n, sizeof(CCBORD *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2873
Status New

	Source	Destination

File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Line	473	473
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
473.                                    sizeof(CCBORD *) * ccba->nalloc,
```

Use of Sizeof On a Pointer Type\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2874
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Line	474	474
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
474.                                    2 * sizeof(CCBORD *) * ccba-
>nalloc)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2875
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1226	1226
Object	sizeof	sizeof

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method	cqcellTreeCreate(void)

```
....
1226.      if ((cqcaa = (CQCELL ***)CALLOC(CQ_NLEVELS + 1, sizeof(CQCELL
**))) == NULL)
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2876
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1230	1230
Object	sizeof	sizeof

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method	cqcellTreeCreate(void)

```
....
1230.          if ((cqca = (CQCELL **)CALLOC(ncells, sizeof(CQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2877
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	2267	2267
Object	sizeof	sizeof

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method	pixOctreeQuantNumColors(PIX *pixs,

```
....
2267.          if ((oqca = (OQCELL **)CALLOC(nbase, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2878
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	2341	2341
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2341.      if ((oqca = (OQCELL **)CALLOC(ncubes, sizeof(OQCELL *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2879
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	2375	2375
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2375.      if ((oqca = (OQCELL **)CALLOC(maxcolors, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2880
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Line	301	301
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Method ccbaCreate(PIX *pixs,

```
....
301.      if ((ccba->ccb = (CCBORD **)CALLOC(n, sizeof(CCBORD *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2881
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Line	473	473
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
473.                                  sizeof(CCBORD *) * ccba->nalloc,
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=2882
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Line	474	474
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
474.                                    2 * sizeof(CCBORD *) * ccba-
>nalloc)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2883
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1226	1226
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1226.      if ((cqcaa = (CQCELL ***)CALLOC(CQ_NLEVELS + 1, sizeof(CQCELL
**))) == NULL)
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2884
Status	New

	Source	Destination

File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1230	1230
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1230.           if ((cqca = (CQCELL **)CALLOC(ncells, sizeof(CQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2885
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	2267	2267
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2267.           if ((oqca = (OQCELL **)CALLOC(nbase, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2886
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	2341	2341

Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2341.       if ((oqca = (OQCELL **)CALLOC(ncubes, sizeof(OQCELL *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2887
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	2375	2375
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2375.       if ((oqca = (OQCELL **)CALLOC(maxcolors, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2888
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Line	301	301
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c

Method	ccbaCreate(PIX *pixs,

```
....
301.      if ((ccba->ccb = (CCBORD **)CALLOC(n, sizeof(CCBORD *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2889
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Line	473	473
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
473.                                    sizeof(CCBORD *) * ccba->nalloc,
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2890
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Line	474	474
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
474.                                    2 * sizeof(CCBORD *) * ccba-
>nalloc)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2891
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1226	1226
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1226.      if ((cqcaa = (CQCELL ***)CALLOC(CQ_NLEVELS + 1, sizeof(CQCELL
**))) == NULL)
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2892
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1230	1230
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1230.          if ((cqca = (CQCELL **)CALLOC(ncells, sizeof(CQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 22:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2893
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	2267	2267
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2267.           if ((oqca = (OQCELL **)CALLOC(nbase, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2894
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	2341	2341
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2341.       if ((oqca = (OQCELL **)CALLOC(ncubes, sizeof(OQCELL *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2895
Status	New

	Source	Destination

File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	2375	2375
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2375.      if ((oqca = (OQCELL **)CALLOC(maxcolors, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2896
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Line	301	301
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Method ccbaCreate(PIX *pixs,

```
....
301.      if ((ccba->ccb = (CCBORD **)CALLOC(n, sizeof(CCBORD *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2897
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Line	473	473

Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
473.                                    sizeof(CCBORD *) * ccba->nalloc,
```

Use of Sizeof On a Pointer Type\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2898
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Line	474	474
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
474.                                    2 * sizeof(CCBORD *) * ccba-
>nalloc)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2899
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Line	1226	1226
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1226.       if ((cqcaa = (CQCELL ***)CALLOC(CQ_NLEVELS + 1, sizeof(CQCELL
**))) == NULL)
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2900
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Line	1230	1230
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1230.           if ((cqca = (CQCELL **)CALLOC(ncells, sizeof(CQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2901
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Line	2267	2267
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2267.           if ((oqca = (OQCELL **)CALLOC(nbase, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2902
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Line	2341	2341
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2341.       if ((oqca = (OQCELL **)CALLOC(ncubes, sizeof(OQCELL *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2903
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Line	2375	2375
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2375.       if ((oqca = (OQCELL **)CALLOC(maxcolors, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 33:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2904
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Line	301	301
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Method ccbaCreate(PIX *pixs,

```
....
301.      if ((ccba->ccb = (CCBORD **)CALLOC(n, sizeof(CCBORD *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2905
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Line	473	473
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
473.                                  sizeof(CCBORD *) * ccba->nalloc,
```

Use of Sizeof On a Pointer Type\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2906
Status	New

	Source	Destination

File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Line	474	474
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
474.                                    2 * sizeof(CCBORD *) * ccba-
>nalloc)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2907
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Line	1226	1226
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1226.      if ((cqcaa = (CQCELL ***)CALLOC(CQ_NLEVELS + 1, sizeof(CQCELL
**))) == NULL)
```

Use of Sizeof On a Pointer Type\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2908
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Line	1230	1230

Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1230.           if ((cqca = (CQCELL **)CALLOC(ncells, sizeof(CQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2909
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Line	2267	2267
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2267.           if ((oqca = (OQCELL **)CALLOC(nbase, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2910
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Line	2341	2341
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c

Method	pixOctreeQuantNumColors(PIX *pixs,

```
....
2341.       if ((oqca = (OQCELL **)CALLOC(ncubes, sizeof(OQCELL *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2911
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Line	2375	2375
Object	sizeof	sizeof

Code Snippet

File Name	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Method	pixOctreeQuantNumColors(PIX *pixs,

```
....
2375.       if ((oqca = (OQCELL **)CALLOC(maxcolors, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2912
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Line	301	301
Object	sizeof	sizeof

Code Snippet

File Name	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Method	ccbaCreate(PIX *pixs,

```
....
301.      if ((ccba->ccb = (CCBORD **)CALLOC(n, sizeof(CCBORD *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2913
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Line	473	473
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
473.                                  sizeof(CCBORD *) * ccba->nalloc,
```

Use of Sizeof On a Pointer Type\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2914
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Line	474	474
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
474.                                  2 * sizeof(CCBORD *) * ccba-
>nalloc)) == NULL)
```

Use of Sizeof On a Pointer Type\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2915
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Line	1226	1226
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1226.       if ((cqcaa = (CQCELL ***)CALLOC(CQ_NLEVELS + 1, sizeof(CQCELL
**))) == NULL)
```

Use of Sizeof On a Pointer Type\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2916
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Line	1230	1230
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1230.           if ((cqca = (CQCELL **)CALLOC(ncells, sizeof(CQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=2917
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Line	2267	2267
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2267.           if ((oqca = (OQCELL **)CALLOC(nbase, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2918
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Line	2341	2341
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2341.       if ((oqca = (OQCELL **)CALLOC(ncubes, sizeof(OQCELL *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2919
Status	New

	Source	Destination

File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Line	2375	2375
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2375.      if ((oqca = (OQCELL **)CALLOC(maxcolors, sizeof(OQCELL *)))
== NULL)
```

Use of Sizeof On a Pointer Type\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2920
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Line	301	301
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Method ccbaCreate(PIX *pixs,

```
....
301.      if ((ccba->ccb = (CCBORD **)CALLOC(n, sizeof(CCBORD *))) ==
NULL)
```

Use of Sizeof On a Pointer Type\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2921
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Line	473	473

Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
473.                                    sizeof(CCBORD *) * ccba->nalloc,
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

NIST SP 800-53: SI-11 Error Handling (P2)

Description

Unchecked Return Value\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2775
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Method ccbaWriteSVGString(const char *filename,

```
....
2513.               sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2776
Status	New

The main method calls the sprintf function, at line 8313 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8654	8654
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8654.       sprintf (ofname+strlen(ofname), "_%0*d",
```

Unchecked Return Value\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2777
Status New

The main method calls the _snprintf function, at line 8313 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8655	8655
Object	_snprintf	_snprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8655.             snprintf(0,0,"%d",is_raw-1), shot_select);
```

Unchecked Return Value\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2778
Status New

The sinar_4shot_load_raw method calls the calloc function, at line 1757 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1772	1772
Object	calloc	calloc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS sinar_4shot_load_raw()

```
....
1772.       calloc ((iheight=height)*(iwidth=width), sizeof *image);
```

Unchecked Return Value\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2779
Status New

The foveon_interpolate method calls the sprintf function, at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3074	3074
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3074.    sprintf (str, "%sRGBNeutral", model2);
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2780

Status	New

The parse_makernote method calls the fgets function, at line 4442 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4546	4546
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_makernote (int base, int uptag)

```
....
4546.         fgets (model2, 64, ifp);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2781
Status	New

The parse_gps method calls the fgets function, at line 4770 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4785	4785
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_gps (int base)

```
....
4785.        fgets ((char *) (gpsdata+14+tag/3), MIN(len,12), ifp);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=2782
Status	New

The parse_tiff_ifd method calls the fgets function, at line 4913 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4977	4977
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4977.       fgets (make, 64, ifp);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2783
Status	New

The parse_tiff_ifd method calls the fgets function, at line 4913 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4980	4980
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4980.       fgets (model, 64, ifp);
```

Unchecked Return Value\Path 10:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2784
Status	New

The parse_tiff_ifd method calls the fgets function, at line 4913 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5011	5011
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5011.       fgets (software, 64, ifp);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2785
Status	New

The parse_tiff_ifd method calls the fgets function, at line 4913 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5076	5076
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5076.       fgets (model2, 64, ifp);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2786
Status	New

The parse_tiff_ifd method calls the sprintf function, at line 4913 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5174	5174
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5174.       sprintf (model, "Ixpress %d-Mp", height*width/1000000);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2787
Status	New

The parse_rollei method calls the fgets function, at line 5659 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5667	5667
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_rollei()

```
....
5667.       fgets (line, 128, ifp);
```

Unchecked Return Value\Path 14:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2788
Status	New

The parse_smal method calls the sprintf function, at line 5889 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5903	5903
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_smal (int offset, int fsize)

```
....
5903.    sprintf (model, "v%d %dx%d", ver, width, height);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2789
Status	New

The parse_cine method calls the sprintf function, at line 5908 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5931	5931
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_cine()

```
....
5931.    sprintf (model, "%d", get4());
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2790
Status	New

The adobe_coeff method calls the sprintf function, at line 6056 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	6489	6489
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS adobe_coeff (char *make, char *model)

```
....
6489.    sprintf (name, "%s %s", make, model);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2791
Status	New

The identify method calls the sprintf function, at line 6544 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7224	7224
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS identify()

```
....
7224.        sprintf (model+20, "DYNAX %-10s", model+6+(model[0]=='M'));
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2792
Status	New

The identify method calls the sprintf function, at line 6544 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7825	7825
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS identify()

```
....
7825.      sprintf (model, "%dx%d", width, height);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2793
Status	New

The tiff_head method calls the sprintf function, at line 8175 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8244	8244
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS tiff_head (struct tiff_hdr *th, int full)

```
....
8244.    sprintf (th->date, "%04d:%02d:%02d %02d:%02d:%02d",
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2794
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Method ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2795
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Method ccbaWriteSVGString(const char *filename,

```
....
2513.               sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2796
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Method ccbaWriteSVGString(const char *filename,

```
....
2513.               sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2797
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c

Method	ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2798
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet	
File Name	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Method	ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2799
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet

File Name	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Method	ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2800
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet	
File Name	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c
Method	ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2801
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c
Method ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2802
Status New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c
Method ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2803
Status New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet	
File Name	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c
Method	ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2804
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet	
File Name	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c
Method	ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2805
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c
Line	2513	2513

Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c
Method ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2806
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c
Line	2513	2513
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c
Method ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2807
Status	New

The ccbaWriteSVGString method calls the sprintf function, at line 2473 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c

Line	2513	2513
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c
Method ccbaWriteSVGString(const char *filename,

```
....
2513.              sprintf(smallbuf, "%0d,%0d", x, y);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2808
Status	New

The main method calls the sprintf function, at line 8313 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8654	8654
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8654.       sprintf (ofname+strlen(ofname), "_%0*d",
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2809
Status	New

The main method calls the _snprintf function, at line 8313 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-	ONLYOFFICE@@core-v99.99.99.2148-

	CVE-2022-29776-FP.c	CVE-2022-29776-FP.c
Line	8655	8655
Object	_snprintf	_snprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8655.             snprintf(0,0,"%d",is_raw-1), shot_select);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2810
Status	New

The sinar_4shot_load_raw method calls the calloc function, at line 1757 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	1772	1772
Object	calloc	calloc

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS sinar_4shot_load_raw()

```
....
1772.       calloc ((iheight=height)*(iwidth=width), sizeof *image);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2811
Status	New

The foveon_interpolate method calls the sprintf function, at line 3014 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3074	3074
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3074.    sprintf (str, "%sRGBNeutral", model2);
```

Unchecked Return Value\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2812
Status New

The parse_makernote method calls the fgets function, at line 4442 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4546	4546
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_makernote (int base, int uptag)

```
....
4546.        fgets (model2, 64, ifp);
```

Unchecked Return Value\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2813
Status New

The parse_gps method calls the fgets function, at line 4770 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4785	4785
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_gps (int base)

```
....
4785.       fgets ((char *) (gpsdata+14+tag/3), MIN(len,12), ifp);
```

Unchecked Return Value\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2814
Status New

The parse_tiff_ifd method calls the fgets function, at line 4913 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4977	4977
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4977.       fgets (make, 64, ifp);
```

Unchecked Return Value\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2815
Status New

The parse_tiff_ifd method calls the fgets function, at line 4913 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4980	4980
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4980.       fgets (model, 64, ifp);
```

Unchecked Return Value\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2816
Status New

The parse_tiff_ifd method calls the fgets function, at line 4913 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5011	5011
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5011.       fgets (software, 64, ifp);
```

Unchecked Return Value\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2817
Status New

The parse_tiff_ifd method calls the fgets function, at line 4913 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5076	5076
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5076.       fgets (model2, 64, ifp);
```

Unchecked Return Value\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2818
Status New

The parse_tiff_ifd method calls the sprintf function, at line 4913 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5174	5174
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5174.       sprintf (model, "Ixpress %d-Mp", height*width/1000000);
```

Unchecked Return Value\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2819
Status New

The parse_rollei method calls the fgets function, at line 5659 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5667	5667
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_rollei()

```
....
5667.      fgets (line, 128, ifp);
```

Unchecked Return Value\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2820
Status New

The parse_smal method calls the sprintf function, at line 5889 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5903	5903
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_smal (int offset, int fsize)

```
....
5903.    sprintf (model, "v%d %dx%d", ver, width, height);
```

Unchecked Return Value\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2821
Status New

The parse_cine method calls the sprintf function, at line 5908 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5931	5931
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_cine()

```
....
5931.    sprintf (model, "%d", get4());
```

Unchecked Return Value\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2822
Status New

The adobe_coeff method calls the sprintf function, at line 6056 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	6489	6489
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS adobe_coeff (char *make, char *model)

```
....
6489.    sprintf (name, "%s %s", make, model);
```

Unchecked Return Value\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2823
Status New

The identify method calls the sprintf function, at line 6544 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7224	7224
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS identify()

```
....
7224.        sprintf (model+20, "DYNAX %-10s", model+6+(model[0]=='M'));
```

Unchecked Return Value\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2824
Status New

The identify method calls the sprintf function, at line 6544 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7825	7825
Object	sprintf	sprintf

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS identify()

```
....
7825.      sprintf (model, "%dx%d", width, height);
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Arithmenic Operation On Boolean\Path 1:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1988
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8432	8432
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8432.         case 'd':  document_mode = 1 + (opt == 'D');
```

Arithmenic Operation On Boolean\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1989
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	334	334
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method double CLASS getreal (int type)

```
....
334.         rev = 7 * ((order == 0x4949) == (ntohs(0x1234) == 0x1234));
```

Arithmenic Operation On Boolean\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1990
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1958	1958
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS olympus_e410_load_raw()

```
....
1958.         i = 2 * (carry[2] < 3);
```

Arithmenic Operation On Boolean\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1991
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3926	3926
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS lin_interpolate()

```
....
3926.          shift = (y==0) + (x==0);
```

Arithmenic Operation On Boolean\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1992
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4866	4866

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4866.      filters = (planes == 1) * 0x01010101 *
```

Arithmenic Operation On Boolean\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1993
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7160	7160
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS identify()

```
....
7160.      load_flags = 6 + (make[0] == 'M');
```

Arithmenic Operation On Boolean\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1994
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7193	7193
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS identify()

```
....
7193.        data_offset += (shot_select > 0) * ( fuji_layout ?
```

Arithmenic Operation On Boolean\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1995
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7224	7224
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS identify()

```
....
7224.        sprintf (model+20, "DYNAX %-10s", model+6+(model[0]=='M'));
```

Arithmenic Operation On Boolean\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1996
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8193	8193
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS tiff_head (struct tiff_hdr *th, int full)

```
....
8193.      tiff_set (&th->ntag, 262, 3, 1, 1 + (colors > 1));
```

Arithmenic Operation On Boolean\Path 10:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1997
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8432	8432
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8432.         case 'd':  document_mode = 1 + (opt == 'D');
```

Arithmenic Operation On Boolean\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1998
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	334	334
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method double CLASS getreal (int type)

```
....
334.         rev = 7 * ((order == 0x4949) == (ntohs(0x1234) == 0x1234));
```

Arithmenic Operation On Boolean\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1999
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	1958	1958
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS olympus_e410_load_raw()

```
....
1958.         i = 2 * (carry[2] < 3);
```

Arithmenic Operation On Boolean\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2000
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3926	3926
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS lin_interpolate()

```
....
3926.          shift = (y==0) + (x==0);
```

Arithmenic Operation On Boolean\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2001
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4866	4866

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4866.       filters = (planes == 1) * 0x01010101 *
```

Arithmenic Operation On Boolean\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2002
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7160	7160
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS identify()

```
....
7160.       load_flags = 6 + (make[0] == 'M');
```

Arithmenic Operation On Boolean\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2003
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7193	7193
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS identify()

```
....
7193.        data_offset += (shot_select > 0) * ( fuji_layout ?
```

Arithmenic Operation On Boolean\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2004
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7224	7224
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS identify()

```
....
7224.        sprintf (model+20, "DYNAX %-10s", model+6+(model[0]=='M'));
```

Arithmenic Operation On Boolean\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2005
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8193	8193
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS tiff_head (struct tiff_hdr *th, int full)

```
....
8193.      tiff_set (&th->ntag, 262, 3, 1, 1 + (colors > 1));
```

Arithmenic Operation On Boolean\Path 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2006
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	756	756
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS canon_compressed_load_raw()

```
....
756.      nblocks = MIN (8, raw_height-row) * raw_width >> 6;
```

Arithmenic Operation On Boolean\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2007
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1033	1033
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS canon_sraw_load_raw()

```
....
1033.      FORC3 rp[c] = CLIP(pix[c] * sraw_mul[c] >> 10);
```

Arithmenic Operation On Boolean\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2008
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1213	1213
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS nikon_compressed_load_raw()

```
....
1213.       BAYER(row,col-left_margin) = curve[LIM((short)hpred[col &
1],0,0x3fff)];
```

Arithmenic Operation On Boolean\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2009
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1465	1465
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS phase_one_flat_field (int is_float, int nc)

```
....
1465.           BAYER(row,col) = LIM(c,0,65535);
```

Arithmenic Operation On Boolean\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2010
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1509	1509

Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS phase_one_correct()

```
....
1509.       curve[i] = LIM(num,0,65535);
```

Arithmenic Operation On Boolean\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2011
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1517	1517
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS phase_one_correct()

```
....
1517.       curve[i] = LIM(num+i,0,65535);
```

Arithmenic Operation On Boolean\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2012
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	1597	1597
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS phase_one_correct()

```
....
1597.       BAYER(row,col) = LIM(i,0,65535);
```

Arithmenic Operation On Boolean\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2013
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2066	2066
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS quicktake_100_load_raw()

```
....
2066.        pixel[row][col] = val = LIM(val,0,255);
```

Arithmenic Operation On Boolean\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2014
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2087	2087
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS quicktake_100_load_raw()

```
....
2087.       pixel[row][col] = val = LIM(val,0,255);
```

Arithmenic Operation On Boolean\Path 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2015
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2095	2095
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS quicktake_100_load_raw()

```
....
2095.         pixel[row][col] = LIM(val,0,255);
```

Arithmenic Operation On Boolean\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2016
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2350	2350
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_yrgb_load_raw()

```
....
2350.         FORC3 image[row*width+col][c] = LIM(rgb[c],0,255);
```

Arithmenic Operation On Boolean\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2017
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2489	2489
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_ycbcr_load_raw()

```
....
2489.           FORC3 ip[c] = curve[LIM(y[j][k]+rgb[c], 0, 0xfff)];
```

Arithmenic Operation On Boolean\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2018
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3717	3717
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS wavelet_denoise()

```
....
3717.         image[i][c] = CLIP(SQR(fimg[i]+fimg[lpass+i])/0x10000);
```

Arithmenic Operation On Boolean\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2019
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3741	3741

Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS wavelet_denoise()

```
....
3741.       BAYER(row,col) = CLIP(SQR(avg+diff) + 0.5);
```

Arithmenic Operation On Boolean\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2020
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3825	3825
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS scale_colors()

```
....
3825.      image[0][i] = CLIP(val);
```

Arithmenic Operation On Boolean\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2021
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4074	4074
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4074.       brow[2][col][c] = CLIP(t);
```

Arithmenic Operation On Boolean\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2022
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4136	4136
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ppg_interpolate()

```
....
4136.       pix[0][c] = CLIP(guess[diff[0] > diff[1]] >> 1);
```

Arithmenic Operation On Boolean\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2023
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4138	4138
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ppg_interpolate()

```
....
4138.       pix[0][c] = CLIP((guess[0]+guess[1]) >> 2);
```

Arithmenic Operation On Boolean\Path 37:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2024
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4204	4204
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ahd_interpolate()

```
....
4204.              rix[0][2-c] = CLIP(val);
```

Arithmenic Operation On Boolean\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2025
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4212	4212
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ahd_interpolate()

```
....
4212.              rix[0][c] = CLIP(val);
```

Arithmenic Operation On Boolean\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2026
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4221	4221
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ahd_interpolate()

```
....
4221.           xyz[0] = cbrt[CLIP((int) xyz[0])];
```

Arithmenic Operation On Boolean\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2027
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4222	4222
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ahd_interpolate()

```
....
4222.           xyz[1] = cbrt[CLIP((int) xyz[1])];
```

Arithmenic Operation On Boolean\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2028
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4223	4223

Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ahd_interpolate()

```
....
4223.           xyz[2] = cbrt[CLIP((int) xyz[2])];
```

Arithmenic Operation On Boolean\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2029
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4242	4242
Object	<	<

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ahd_interpolate()

```
....
4242.         leps = MIN(MAX(ldiff[0][0],ldiff[0][1]),
```

Arithmenic Operation On Boolean\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2030
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4244	4244
Object	<	<

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ahd_interpolate()

```
....
4244.          abeps = MIN(MAX(abdiff[0][0],abdiff[0][1]),
```

Arithmenic Operation On Boolean\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2031
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4295	4295
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS median_filter()

```
....
4295.        pix[0][c] = CLIP(med[4] + pix[0][1]);
```

Arithmenic Operation On Boolean\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2032
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4407	4407
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS recover_highlights()

```
....
4407.              if (pixel[c] < val) pixel[c] = CLIP(val);
```

Arithmenic Operation On Boolean\Path 46:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2033
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8018	8018
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS convert_to_rgb()

```
....
8018.       FORC3 img[c] = CLIP((int) out[c]);
```

Arithmenic Operation On Boolean\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2034
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	756	756
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS canon_compressed_load_raw()

```
....
756.      nblocks = MIN (8, raw_height-row) * raw_width >> 6;
```

Arithmenic Operation On Boolean\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2035
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	1033	1033
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS canon_sraw_load_raw()

```
....
1033.       FORC3 rp[c] = CLIP(pix[c] * sraw_mul[c] >> 10);
```

Arithmenic Operation On Boolean\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2036
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	1213	1213
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS nikon_compressed_load_raw()

```
....
1213.       BAYER(row,col-left_margin) = curve[LIM((short)hpred[col &
1],0,0x3fff)];
```

Arithmenic Operation On Boolean\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2037
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	1465	1465

Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS phase_one_flat_field (int is_float, int nc)

```
....
1465.           BAYER(row,col) = LIM(c,0,65535);
```

TOCTOU

Query Path:
CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2715
Status New

The ccbaWrite method in ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2716
Status New

The ccbaRead method in ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2717
Status New

The main method in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8473	8473
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8473.       if (!(ifp = fopen (ifname, "rb"))) {
```

TOCTOU\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2718
Status New

The main method in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8659	8659
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8659.         ofp = fopen (ofname, "wb");
```

TOCTOU\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2719
Status New

The bad_pixels method in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3425	3425
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3425.       fp = fopen (fname, "r");
```

TOCTOU\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2720
Status New

The bad_pixels method in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3444	3444
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3444.         if ((fp = fopen (fname, "r"))) break;
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2721
Status	New

The subtract method in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3482	3482
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS subtract (char *fname)

```
....
3482.     if (!(fp = fopen (fname, "rb"))) {
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2722
Status	New

The parse_external_jpeg method in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5512	5512
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_external_jpeg()

```
....
5512.      if ((ifp = fopen (jname, "rb"))) {
```

TOCTOU\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2723
Status New

The apply_profile method in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7883	7883
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7883.    else if ((fp = fopen (output, "rb"))) {
```

TOCTOU\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2724
Status New

The ccbaWrite method in ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2725
Status New

The ccbaRead method in ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2726
Status New

The ccbaWrite method in ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2727
Status New

The ccbaRead method in ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2728
Status New

The ccbaWrite method in ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2729
Status New

The ccbaRead method in ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2730
Status New

The ccbaWrite method in ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2731
Status New

The ccbaRead method in ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2732
Status New

The ccbaWrite method in ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2733
Status New

The ccbaRead method in ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2734
Status New

The ccbaWrite method in ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2735
Status New

The ccbaRead method in ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2736
Status New

The ccbaWrite method in ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2737
Status New

The ccbaRead method in ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2738
Status New

The ccbaWrite method in ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2739
Status	New

The ccbaRead method in ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2740
Status	New

The ccbaWrite method in ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2741
Status New

The ccbaRead method in ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2742
Status New

The ccbaWrite method in ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2743
Status New

The ccbaRead method in ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2744
Status New

The ccbaWrite method in ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2745
Status New

The ccbaRead method in ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2746
Status New

The ccbaWrite method in ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2747
Status New

The ccbaRead method in ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2748
Status New

The ccbaWrite method in ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2749
Status New

The ccbaRead method in ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2750
Status New

The ccbaWrite method in ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2751
Status New

The ccbaRead method in ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2752
Status New

The main method in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8473	8473
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8473.       if (!(ifp = fopen (ifname, "rb"))) {
```

TOCTOU\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2753
Status	New

The main method in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8659	8659
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8659.         ofp = fopen (ofname, "wb");
```

TOCTOU\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2754
Status	New

The bad_pixels method in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3425	3425
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3425.       fp = fopen (fname, "r");
```

TOCTOU\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2755
Status	New

The bad_pixels method in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3444	3444
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3444.         if ((fp = fopen (fname, "r"))) break;
```

TOCTOU\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2756
Status	New

The subtract method in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3482	3482
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS subtract (char *fname)

```
....
3482.    if (!(fp = fopen (fname, "rb"))) {
```

TOCTOU\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2757
Status	New

The parse_external_jpeg method in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5512	5512
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_external_jpeg()

```
....
5512.      if ((ifp = fopen (jname, "rb"))) {
```

TOCTOU\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2758
Status	New

The apply_profile method in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7883	7883
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7883.    else if ((fp = fopen (output, "rb"))) {
```

TOCTOU\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2759
Status	New

The ccbaWrite method in ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2760
Status	New

The ccbaRead method in ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.      if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2761
Status	New

The CFileBinary::OpenFile method in ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Line	945	945
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Method bool CFileBinary::OpenFile(const std::wstring& sFileName, bool bRewrite)

```
....
945.          m_pFile = fopen(fileSystemRepresentation(sFileName),
bRewrite ? "rb+" : "rb");
```

TOCTOU\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2762
Status	New

The CFileBinary::CreateFileW method in ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Line	979	979
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Method bool CFileBinary::CreateFileW(const std::wstring& sFileName)

```
....
979.            m_pFile = fopen(fileSystemRepresentation(sFileName),
"wb");
```

TOCTOU\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2763
Status New

The CFileBinary::OpenFile method in ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c
Line	945	945
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c
Method bool CFileBinary::OpenFile(const std::wstring& sFileName, bool bRewrite)

```
....
945.            m_pFile = fopen(fileSystemRepresentation(sFileName),
bRewrite ? "rb+" : "rb");
```

TOCTOU\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=2764
Status	New

The CFileBinary::CreateFileW method in ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c
Line	979	979
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2022-29776-FP.c
Method bool CFileBinary::CreateFileW(const std::wstring& sFileName)

```
....
979.            m_pFile = fopen(fileSystemRepresentation(sFileName),
"wb");
```

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=1020062&projectid=20045&pathid=2618
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2619
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.      if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2620
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8473	8473
Object	ifp	ifp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8473.      if (!(ifp = fopen (ifname, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2621
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8659	8659
Object	ofp	ofp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8659.         ofp = fopen (ofname, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2622
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3425	3425
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3425.       fp = fopen (fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2623
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3444	3444
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3444.        if ((fp = fopen (fname, "r"))) break;
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2624
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3482	3482
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS subtract (char *fname)

```
....
3482.    if (!(fp = fopen (fname, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2625
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5512	5512

Object	ifp	ifp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_external_jpeg()

```
....
5512.      if ((ifp = fopen (jname, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2626
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7883	7883
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7883.    else if ((fp = fopen (output, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2627
Status New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2628
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.      if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2629
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2630
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2631
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2632
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2633
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2634
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Line	2287	2287

Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2635
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2636
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2637
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2638
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2639
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2640
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2641
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2642
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2643
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c
Line	2140	2140

Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2644
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.      if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2645
Status New

	Source	Destination
File	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2646
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.      if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2647
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 31:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2648
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2649
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2650
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2651
Status New

	Source	Destination
File	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2652
Status New

	Source	Destination
File	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c
Line	2287	2287

Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.      if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2653
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2654
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.      if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2655
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8473	8473
Object	ifp	ifp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8473.      if (!(ifp = fopen (ifname, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2656
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8659	8659
Object	ofp	ofp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8659.        ofp = fopen (ofname, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 40:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2657
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3425	3425
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3425.       fp = fopen (fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2658
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3444	3444
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3444.         if ((fp = fopen (fname, "r"))) break;
```

Incorrect Permission Assignment For Critical Resources\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2659
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3482	3482
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS subtract (char *fname)

```
....
3482.    if (!(fp = fopen (fname, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2660
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5512	5512
Object	ifp	ifp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_external_jpeg()

```
....
5512.      if ((ifp = fopen (jname, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2661
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7883	7883

Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7883.    else if ((fp = fopen (output, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2662
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2663
Status New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c
Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.      if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2664
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2022-29776-FP.c
Line	1526	1526
Object	CreateFileW	CreateFileW

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2022-29776-FP.c
Method unsigned long CFileBinary::GetDateTime(const std::wstring & inputFile)

```
....
1526.          hFile = ::CreateFileW(inputFile.c_str(), GENERIC_READ,
FILE_SHARE_READ,  NULL,  OPEN_EXISTING,  FILE_ATTRIBUTE_NORMAL, NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2665
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Line	1189	1189
Object	CreateFileW	CreateFileW

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Method bool CFileBinary::SaveToFile(const std::wstring& strFileName, const std::wstring& strXml, bool bIsBOM)

```
....
1189.          oFile.CreateFileW(strFileName);
```

Incorrect Permission Assignment For Critical Resources\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2666
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Line	1340	1340
Object	CreateFileW	CreateFileW

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Method bool CFileBinary::Truncate(const std::wstring& sPath, size_t nNewSize)

```
....
1340.           HANDLE hFile = ::CreateFileW( sPath.c_str(),
GENERIC_WRITE, FILE_SHARE_READ,
```

Incorrect Permission Assignment For Critical Resources\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2667
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Line	1526	1526
Object	CreateFileW	CreateFileW

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2022-29776-FP.c
Method unsigned long CFileBinary::GetDateTime(const std::wstring & inputFile)

```
....
1526.           hFile = ::CreateFileW(inputFile.c_str(), GENERIC_READ,
FILE_SHARE_READ,  NULL,  OPEN_EXISTING,  FILE_ATTRIBUTE_NORMAL, NULL);
```

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=1020062&projectid=20045&pathid=1220
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1221
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1222
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 972 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	983	983
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS canon_sraw_load_raw()

```
....
983.    for (ecol=slice=0; slice <= cr2_slice[0]; slice++) {
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1223
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 2166 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	2185	2185
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2185.        for (r=0; r <= !c; r++) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1224
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3962 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3999	3999
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
3999.    for (row=0; row <= prow; row++)        /* Precalculate for VNG
*/
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1225
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3962 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4000	4000
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4000.       for (col=0; col <= pcol; col++) {
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1226
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 4148 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4258	4258
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS ahd_interpolate()

```
....
4258.           for (hm[d]=0, i=tr-1; i <= tr+1; i++)
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1227
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 4273 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	4289	4289
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS median_filter()

```
....
4289.       for (k=0, i = -width; i <= width; i += width)
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1228
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1229
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v6.3.0.70-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1230
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1231
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v6.4.0.85-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1232
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1233
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.0.0.27-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1234
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1235
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.201-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1236
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1237
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.1.0.46-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1238
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1239
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.2.0.130-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1240
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1241
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.3.0.5-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1242
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1243
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.3.3.6-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1244
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1245
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.4.0.101-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1246
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1247
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.5.0.22-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1248
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1249
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v7.6.0.2-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1250
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1251
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v8.0.1.26-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1252
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1253
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v8.1.0.126-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1254
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1255
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1256
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 972 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	983	983
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS canon_sraw_load_raw()

```
....
983.     for (ecol=slice=0; slice <= cr2_slice[0]; slice++) {
```

Potential Off by One Error in Loops\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1257
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 2166 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	2185	2185
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2185.        for (r=0; r <= !c; r++) {
```

Potential Off by One Error in Loops\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1258
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 3962 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3999	3999
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
3999.    for (row=0; row <= prow; row++)        /* Precalculate for VNG
*/
```

Potential Off by One Error in Loops\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1259
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 3962 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4000	4000
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4000.       for (col=0; col <= pcol; col++) {
```

Potential Off by One Error in Loops\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1260
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 4148 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4258	4258
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS ahd_interpolate()

```
....
4258.           for (hm[d]=0, i=tr-1; i <= tr+1; i++)
```

Potential Off by One Error in Loops\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1261
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 4273 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	4289	4289
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS median_filter()

```
....
4289.       for (k=0, i = -width; i <= width; i += width)
```

Potential Off by One Error in Loops\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1262
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36281-TP.c at line 1217 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1263
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36281-TP.c at line 1250 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2268-CVE-2020-36281-TP.c
Method cqcellTreeDestroy(CQCELL ****pcqcaa)

```
....
1266.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Heuristic 2nd Order Buffer Overflow malloc

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow malloc Version:0

Categories

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

Description

Heuristic 2nd Order Buffer Overflow malloc\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1974
Status	New

The size of the buffer used by foveon_thumb in bwide, at line 2803 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get4 passes to str, at line 299 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	302	2814
Object	str	bwide

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method unsigned CLASS get4()

```
....
302.    fread (str, 1, 4, ifp);
```

File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_thumb (FILE *tfp)

```
....
2814.       buf = (char *) malloc (bwide);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1975
Status	New

The size of the buffer used by apply_profile in size, at line 7860 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that apply_profile passes to Address, at line 7860 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7884	7886
Object	Address	size

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7884.       fread (&size, 4, 1, fp);
....
7886.       oprof = (unsigned *) malloc (size = ntohl(size));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1976
Status	New

The size of the buffer used by foveon_thumb in bwide, at line 2803 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get4 passes to str, at line 299 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	302	2814
Object	str	bwide

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method unsigned CLASS get4()

```
....
302.    fread (str, 1, 4, ifp);
```

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS foveon_thumb (FILE *tfp)

```
....
2814.      buf = (char *) malloc (bwide);
```

Heuristic 2nd Order Buffer Overflow malloc\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1977
Status	New

The size of the buffer used by apply_profile in size, at line 7860 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that apply_profile passes to Address, at line 7860 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7884	7886
Object	Address	size

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	void CLASS apply_profile (char *input, char *output)

```
....
7884.      fread (&size, 4, 1, fp);
....
7886.      oprof = (unsigned *) malloc (size = ntohl(size));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1978
Status	New

The size of the buffer used by apply_profile in ntohl, at line 7860 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that apply_profile passes to Address, at line 7860 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7884	7886

Object	Address	ntohl

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7884.       fread (&size, 4, 1, fp);
....
7886.       oprof = (unsigned *) malloc (size = ntohl(size));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1979
Status New

The size of the buffer used by apply_profile in ntohl, at line 7860 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that apply_profile passes to Address, at line 7860 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7884	7886
Object	Address	ntohl

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7884.       fread (&size, 4, 1, fp);
....
7886.       oprof = (unsigned *) malloc (size = ntohl(size));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1980
Status New

The size of the buffer used by apply_profile in size, at line 7860 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that apply_profile passes to Address, at line 7860 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	7884	7886
Object	Address	size

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7884.       fread (&size, 4, 1, fp);
....
7886.       oprof = (unsigned *) malloc (size = ntohl(size));
```

Heuristic 2nd Order Buffer Overflow malloc\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1981
Status	New

The size of the buffer used by apply_profile in size, at line 7860 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that apply_profile passes to Address, at line 7860 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	7884	7886
Object	Address	size

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7884.       fread (&size, 4, 1, fp);
....
7886.       oprof = (unsigned *) malloc (size = ntohl(size));
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:
CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2707
Status	New

The system data read by main in the file ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8455	8455
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8455.         perror ("setmode()");
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2708
Status	New

The system data read by main in the file ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8474	8474
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8474.        perror (ifname);
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2709
Status	New

The system data read by main in the file ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8662	8662
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8662.        perror (ofname);
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2710
Status	New

The system data read by subtract in the file ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3476 is potentially exposed by subtract found in ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c at line 3476.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3483	3483
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c

Method	void CLASS subtract (char *fname)

```
....
3483.      perror (fname);  return;
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2711
Status	New

The system data read by main in the file ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8455	8455
Object	perror	perror

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	int CLASS main (int argc, char **argv)

```
....
8455.        perror ("setmode()");
```

Exposure of System Data to Unauthorized Control Sphere\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2712
Status	New

The system data read by main in the file ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8474	8474
Object	perror	perror

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	int CLASS main (int argc, char **argv)

```
....
8474.        perror (ifname);
```

Exposure of System Data to Unauthorized Control Sphere\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2713
Status	New

The system data read by main in the file ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8662	8662
Object	perror	perror

Code Snippet

File Name	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method	int CLASS main (int argc, char **argv)

```
....
8662.        perror (ofname);
```

Exposure of System Data to Unauthorized Control Sphere\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2714
Status	New

The system data read by subtract in the file ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 3476 is potentially exposed by subtract found in ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c at line 3476.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3483	3483
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS subtract (char *fname)

```
....
3483.      perror (fname);  return;
```

Potential Precision Problem

Query Path:
CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Precision Problem\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1982
Status	New

The size of the buffer used by parse_riff in "%*s %s %d %d:%d:%d %d", at line 5849 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_riff passes to "%*s %s %d %d:%d:%d %d", at line 5849 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5877	5877
Object	"%*s %s %d %d:%d:%d %d"	"%*s %s %d %d:%d:%d %d"

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS parse_riff()

```
....
5877.      if (sscanf (date, "%*s %s %d %d:%d:%d %d", month, &t.tm_mday,
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1983
Status	New

The size of the buffer used by parse_riff in "%*s %s %d %d:%d:%d %d", at line 5849 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parse_riff passes to "%*s %s %d %d:%d:%d %d", at line 5849 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5877	5877
Object	"%*s %s %d %d:%d:%d %d"	"%*s %s %d %d:%d:%d %d"

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS parse_riff()

```
....
5877.      if (sscanf (date, "%*s %s %d %d:%d:%d %d", month, &t.tm_mday,
```

Potential Precision Problem\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1984
Status New

The size of the buffer used by foveon_interpolate in "%sRGBNeutral", at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that foveon_interpolate passes to "%sRGBNeutral", at line 3014 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	3074	3074
Object	"%sRGBNeutral"	"%sRGBNeutral"

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3074.    sprintf (str, "%sRGBNeutral", model2);
```

Potential Precision Problem\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20

	045&pathid=1985
Status	New

The size of the buffer used by adobe_coeff in "%s %s", at line 6056 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that adobe_coeff passes to "%s %s", at line 6056 of ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	6489	6489
Object	"%s %s"	"%s %s"

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method void CLASS adobe_coeff (char *make, char *model)

```
....
6489.    sprintf (name, "%s %s", make, model);
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1986
Status	New

The size of the buffer used by foveon_interpolate in "%sRGBNeutral", at line 3014 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that foveon_interpolate passes to "%sRGBNeutral", at line 3014 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	3074	3074
Object	"%sRGBNeutral"	"%sRGBNeutral"

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3074.    sprintf (str, "%sRGBNeutral", model2);
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=1987
Status	New

The size of the buffer used by adobe_coeff in "%s %s", at line 6056 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that adobe_coeff passes to "%s %s", at line 6056 of ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	6489	6489
Object	"%s %s"	"%s %s"

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method void CLASS adobe_coeff (char *make, char *model)

```
....
6489.    sprintf (name, "%s %s", make, model);
```

Insecure Temporary File

Query Path:
CPP\Cx\CPP Low Visibility\Insecure Temporary File Version:0

Categories

NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Insecure Temporary File\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2062
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	5295	5295
Object	tmpfile	tmpfile

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5295.       if ((ifp = tmpfile())) {
```

Insecure Temporary File\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2063
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	5295	5295
Object	tmpfile	tmpfile

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5295.       if ((ifp = tmpfile())) {
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2064
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Line	8588	8588
Object	cmatrix	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.99.2024-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8588.        memcpy (rgb_cam, cmatrix, sizeof cmatrix);
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2065
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Line	8588	8588
Object	cmatrix	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v99.99.99.2148-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8588.        memcpy (rgb_cam, cmatrix, sizeof cmatrix);
```

Use of Insufficiently Random Values

Query Path:
CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Insufficiently Random Values\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2773
Status	New

Method myrand at line 2412 of OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Line	2422	2422

Object	rand	rand

Code Snippet
File Name OP-TEE@@optee_os-4.0.0-rc1-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2422.           output[i] = rand();
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020062&projectid=20045&pathid=2774
Status	New

Method myrand at line 2412 of OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c	OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c
Line	2422	2422
Object	rand	rand

Code Snippet
File Name OP-TEE@@optee_os-4.1.0-CVE-2024-23170-TP.c
Method static int myrand(void *rng_state, unsigned char *output, size_t len)

```
....
2422.           output[i] = rand();
```

Buffer Overflow cpycat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow Indexes

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Format String Attack

Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

Cause

How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

General Recommendations

How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
- Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.

Source Code Examples

CPP

Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or
```

```
cause a crash
```

Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

---

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
	int i;
	i = 1;
	return &i;
}

void func2()
```

```
{
	int j;
	j = 5;
}

//..
	int * i = func1();
	printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
	func2();
	printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow 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
```

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

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Char 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;
}
```

Float 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

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

Short 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

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;
}
```

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Stored Buffer Overflow boundcpy

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
```

```
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Stored Buffer Overflow cpycat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In 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

Uncontrolled Recursion

Weakness ID: 674 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product does not properly control the amount of recursion that takes place, which consumes excessive resources, such as allocated memory or the program stack.

Alternate Terms

Stack Exhaustion

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

Scope	Effect
Availability	Resources including CPU, memory, and stack memory could be rapidly consumed or exhausted, eventually leading to an exit or crash.
Confidentiality	In some cases, an application's interpreter might kill a process or thread that appears to be consuming too much resources, such as with PHP's memory_limit setting. When the interpreter kills the process/thread, it might report an error containing detailed information such as the application's installation path.

Observed Examples

Reference	Description
CVE-2007-1285	Deeply nested arrays trigger stack exhaustion.
CVE-2007-3409	Self-referencing pointers create infinite loop and resultant stack exhaustion.

Potential Mitigations

Limit the number of recursive calls to a reasonable number.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Development Concepts (primary)699**
ChildOf	Weakness Class	691	Insufficient Control Flow Management	**Research Concepts (primary)1000**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**

Affected Resources

- CPU

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
82	Violating Implicit Assumptions Regarding XML Content (aka XML Denial of Service (XDoS))	
99	XML Parser Attack	

Content History

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Common Consequences, Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

BACK TO TOP

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Heuristic 2nd Order Buffer Overflow malloc

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

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Code Quality		

BACK TO TOP

Insecure Temporary File

Weakness ID: 377 *(Weakness Base)* **Status:** Incomplete

Description

Description Summary

Creating and using insecure temporary files can leave application and system data vulnerable to attack.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Demonstrative Examples

Example 1

The following code uses a temporary file for storing intermediate data gathered from the network before it is processed.

(Bad Code)

Example Language: **C**

```
if (tmpnam_r(filename)) {

FILE* tmp = fopen(filename,"wb+");
while((recv(sock,recvbuf,DATA_SIZE, 0) > 0)&(amt!=0)) amt = fwrite(recvbuf,1,DATA_SIZE,tmp);
}
...
```

This otherwise unremarkable code is vulnerable to a number of different attacks because it relies on an insecure method for creating temporary files. The vulnerabilities introduced by this function and others are described in the following sections. The most egregious security problems related to temporary file creation have occurred on Unix-based operating systems, but Windows applications have parallel risks. This section includes a discussion of temporary file creation on both Unix and Windows systems. Methods and behaviors can vary between systems, but the fundamental risks introduced by each are reasonably constant.

Other Notes

Applications require temporary files so frequently that many different mechanisms exist for creating them in the C Library and Windows(R) API. Most of these functions are vulnerable to various forms of attacks.

The functions designed to aid in the creation of temporary files can be broken into two groups based whether they simply provide a filename or actually open a new file. - Group 1: "Unique" Filenames: The first group of C Library and WinAPI functions designed to help with the process of creating temporary files do so by generating a unique file name for a new temporary file, which the program is then supposed to open. This group includes C Library functions like tmpnam(), tempnam(), mktemp() and their C++ equivalents prefaced with an _ (underscore) as well as the GetTempFileName() function from the Windows API. This group of functions suffers from an underlying race condition on the filename chosen. Although the functions guarantee that the filename is unique at the time it is selected, there is no mechanism to prevent another process or an attacker from creating a file with the same name after it is selected but before the application attempts to open the file. Beyond the risk of a legitimate collision caused by another call to the same function, there is a high probability that an attacker will be able to create a malicious collision because the filenames generated by these functions are not sufficiently randomized to make them difficult to guess. If a file with the selected name is created, then depending on how the file is opened the existing contents or access permissions of the file may remain intact. If the existing contents of the file are malicious in nature, an attacker may be able to inject dangerous data into the application when it reads data back from the temporary file. If an attacker pre-creates the file with relaxed access permissions, then data stored in the temporary file by the application may be accessed, modified or corrupted by an attacker. On Unix based systems an even more insidious attack is possible if the attacker pre-creates the file as a link to another important file. Then, if the application truncates or writes data to the file, it may unwittingly perform damaging operations for the attacker. This is an especially serious threat if the program operates with elevated permissions. Finally, in the best case the file will be opened with the a call to open() using the O_CREAT and O_EXCL flags or to CreateFile() using the CREATE_NEW attribute, which will fail if the file already exists and therefore prevent the types of attacks described above. However, if an attacker is able to accurately predict a sequence of temporary file names, then the application may be prevented from opening necessary temporary storage causing a denial of service (DoS) attack. This type of attack would not be difficult to mount given the small amount of randomness used in

the selection of the filenames generated by these functions. - Group 2: "Unique" Files: The second group of C Library functions attempts to resolve some of the security problems related to temporary files by not only generating a unique file name, but also opening the file. This group includes C Library functions like tmpfile() and its C++ equivalents prefaced with an _ (underscore), as well as the slightly better-behaved C Library function mkstemp(). The tmpfile() style functions construct a unique filename and open it in the same way that fopen() would if passed the flags "wb+", that is, as a binary file in read/write mode. If the file already exists, tmpfile() will truncate it to size zero, possibly in an attempt to assuage the security concerns mentioned earlier regarding the race condition that exists between the selection of a supposedly unique filename and the subsequent opening of the selected file. However, this behavior clearly does not solve the function's security problems. First, an attacker can pre-create the file with relaxed access-permissions that will likely be retained by the file opened by tmpfile(). Furthermore, on Unix based systems if the attacker pre-creates the file as a link to another important file, the application may use its possibly elevated permissions to truncate that file, thereby doing damage on behalf of the attacker. Finally, if tmpfile() does create a new file, the access permissions applied to that file will vary from one operating system to another, which can leave application data vulnerable even if an attacker is unable to predict the filename to be used in advance. Finally, mkstemp() is a reasonably safe way create temporary files. It will attempt to create and open a unique file based on a filename template provided by the user combined with a series of randomly generated characters. If it is unable to create such a file, it will fail and return -1. On modern systems the file is opened using mode 0600, which means the file will be secure from tampering unless the user explicitly changes its access permissions. However, mkstemp() still suffers from the use of predictable file names and can leave an application vulnerable to denial of service attacks if an attacker causes mkstemp() to fail by predicting and pre-creating the filenames to be used.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	361	Time and State	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	376	Temporary File Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ParentOf	Weakness Base	378	Creation of Temporary File With Insecure Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	379	Creation of Temporary File in Directory with Incorrect Permissions	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Insecure Temporary File

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 23, "Creating Temporary Files Securely" Page 682. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated References		

BACK TO TOP

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
           incrementCounter ic;
           decrementCounter dc;
           while(counter == 0) { // because of proper locking, this condition is never false
                  counter = 0;
                  ic = new incrementCounter();
                  dc = new decrementCounter();
                  ic.start();
                  dc.start();
                  ic.join();
                  dc.join();
           }
           System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter--;
           }
        }
    }
```

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.
Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

```
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Scanned Languages

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