vul_files_38 Scan Report

Project Name	vul_files_38
Scan Start	Tuesday, January 7, 2025 8:30:21 PM
Preset	Checkmarx Default
Scan Time	04h:21m:19s
Lines Of Code Scanned	299886
Files Scanned	89
Report Creation Time	Wednesday, January 8, 2025 9:52:28 AM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	2/100 (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

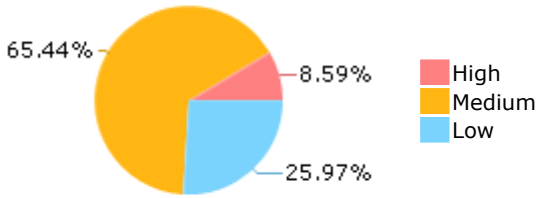
Results Limit

Results limit per query was set to 50

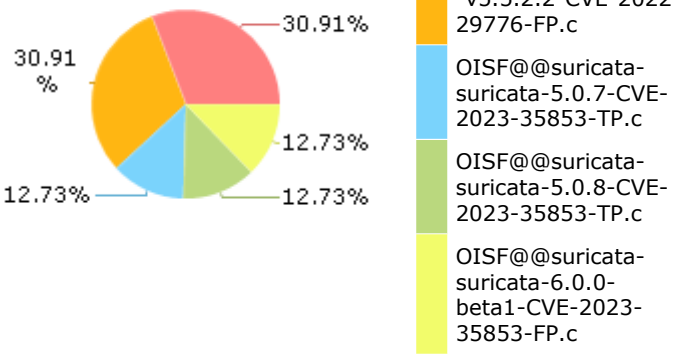
Selected Queries

Selected queries are listed in Result Summary

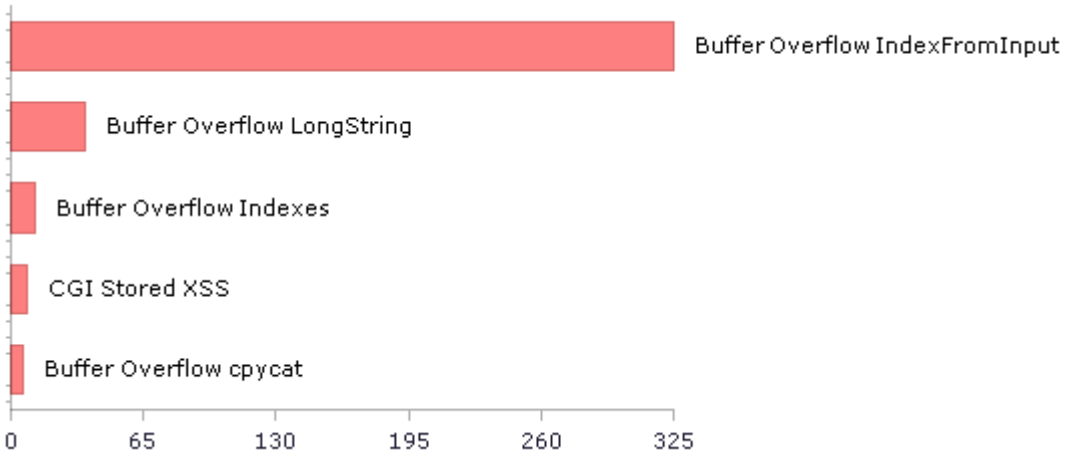
Result Summary



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	1648	1163
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	645	645
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	2	2
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	8	4
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	1624	1624
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	8	4
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	1624	1624
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	18	18
PCI DSS (3.2) - 6.5.2 - Buffer overflows	1201	1088
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)	8	4
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.	126	126
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.	519	519
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	45	41

***** 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)	653	653
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	2	2
SC-5 Denial of Service Protection (P1)*	314	193
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	248	188
SI-11 Error Handling (P2)*	190	190
SI-15 Information Output Filtering (P0)	8	4
SI-16 Memory Protection (P1)	145	53

***** 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

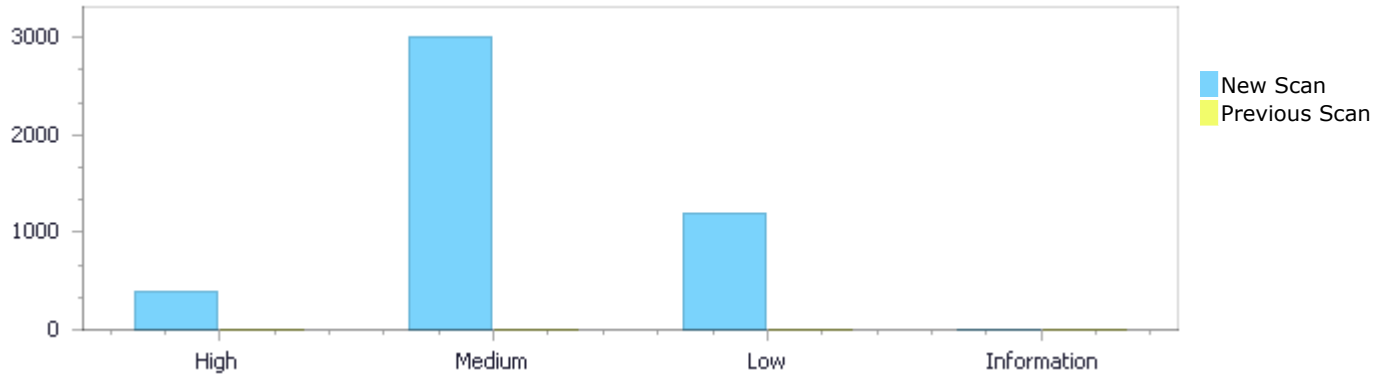
Scan Summary - Custom

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	395	3,009	1,194	0	4,598
Recurrent Issues	0	0	0	0	0
Total	395	3,009	1,194	0	4,598
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	395	3,009	1,194	0	4,598
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	395	3,009	1,194	0	4,598

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	325	High
Buffer Overflow LongString	36	High
Buffer Overflow Indexes	12	High
CGI Stored XSS	8	High
Buffer Overflow cpycat	6	High

Buffer Overflow StrcpyStrcat	6	High
Format String Attack	2	High
Dangerous Functions	1624	Medium
Buffer Overflow boundcpy WrongSizeParam	967	Medium
Buffer Overflow Loops	120	Medium
Use of Zero Initialized Pointer	76	Medium
Stored Buffer Overflow boundcpy	38	Medium
Divide By Zero	29	Medium
Use of Uninitialized Variable	28	Medium
Use of Uninitialized Pointer	24	Medium
Wrong Size t Allocation	18	Medium
Memory Leak	17	Medium
Integer Overflow	15	Medium
Float Overflow	12	Medium
MemoryFree on StackVariable	12	Medium
Short Overflow	10	Medium
Stored Buffer Overflow cpycat	6	Medium
Buffer Overflow AddressOfLocalVarReturned	4	Medium
Double Free	4	Medium
Off by One Error in Loops	2	Medium
Uncontrolled Recursion	2	Medium
Off by One Error in Methods	1	Medium
Improper Resource Access Authorization	519	Low
Unchecked Return Value	190	Low
Incorrect Permission Assignment For Critical Resources	126	Low
NULL Pointer Dereference	91	Low
Unchecked Array Index	91	Low
Arithmenic Operation On Boolean	74	Low
Use of Sizeof On a Pointer Type	29	Low
TOCTOU	27	Low
Potential Off by One Error in Loops	18	Low
Exposure of System Data to Unauthorized Control Sphere	8	Low
Heuristic 2nd Order Buffer Overflow malloc	8	Low
Potential Precision Problem	6	Low
Sizeof Pointer Argument	5	Low
Insecure Temporary File	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	477
ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	477
OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	317
OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	317
OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	317
OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c	317
OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c	317
ntop@@nDPI-3.2-CVE-2020-15475-TP.c	81
OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	22

nothings@@stb-newest-CVE-2021-3520-FP.c	22

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=1020047&projectid=20040&pathid=55
Status	New

The size of the buffer used by main in argc, at line 8313 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8313	8381
Object	argc	argc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=56
Status	New

The size of the buffer used by main in argc, at line 8313 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination

File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8313	8381
Object	argc	argc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=57
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4831	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=58
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4842	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=59
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4846	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=60
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4848	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=61
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4851	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=62
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4855	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=63
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=64
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=65
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-	ONLYOFFICE@@core-v5.4.99.1786-CVE-

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

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=66
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4831	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=67
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4842	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=68
Status New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4846	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20

	040&pathid=69
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4848	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=70
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4848	4867
Object	Address	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=71
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4831	4802
Object	ifp	i

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method void CLASS parse_mos (int offset)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=72
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4842	4802
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=73
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	338	4802
Object	fgetc	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method double CLASS getreal (int type)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=74
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	286	4802
Object	str	i

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method ushort CLASS get2()

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=75
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	302	4802
Object	str	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method unsigned CLASS get4()

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=76
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4842	4802
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 23:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=77
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4831	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=78
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4842	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=79
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4846	4833
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=80
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4848	4833
Object	ifp	i

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.2.2-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 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=81
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4851	4833
Object	ifp	i

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.2.2-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 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=82
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-	ONLYOFFICE@@core-v5.5.2.2-CVE-

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

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=83
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=84
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 31:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=85
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 32:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=86
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4831	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=87
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4842	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=88
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4846	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=89
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4848	4867
Object	ifp	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=90
Status	New

The size of the buffer used by parse_mos in BinaryExpr, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4848	4867
Object	Address	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=91
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4831	4802
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=92
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4842	4802
Object	ifp	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=93
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	338	4802
Object	fgetc	i

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method double CLASS getreal (int type)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=94
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	286	4802
Object	str	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method ushort CLASS get2()

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

File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=95
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	302	4802
Object	str	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method unsigned CLASS get4()

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

File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=96
Status	New

The size of the buffer used by romm_coeff in i, at line 4791 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4842	4802
Object	Address	i

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method void CLASS parse_mos (int offset)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=97
Status	New

The size of the buffer used by ndpi_load_protocols_file in i, at line 2911 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ndpi_load_protocols_file passes to fgets, at line 2911 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	2935	2949
Object	fgets	i

Code Snippet

File Name	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method	int ndpi_load_protocols_file(struct ndpi_detection_module_struct *ndpi_str, const char* path) {

```
....
2935.      while((line = fgets(line, line_len, fd)) != NULL &&
line[strlen(line)-1] != '\n') {
....
2949.        line = &buffer[i];
```

Buffer Overflow IndexFromInput\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=98
Status	New

The size of the buffer used by phase_one_correct in i, at line 1479 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	338	1579
Object	fgetc	i

Code Snippet

File Name	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method	double CLASS getreal (int type)

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

File Name	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method	void CLASS phase_one_correct()

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

Buffer Overflow IndexFromInput\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=99
Status	New

The size of the buffer used by phase_one_correct in i, at line 1479 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	286	1579
Object	str	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method ushort CLASS get2()

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

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS phase_one_correct()

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

Buffer Overflow IndexFromInput\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=100
Status	New

The size of the buffer used by phase_one_correct in i, at line 1479 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	302	1579
Object	str	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method unsigned CLASS get4()

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=101
Status	New

The size of the buffer used by quicktake_100_load_raw in getbits, at line 2036 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2086
Object	fgetc	getbits

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method void CLASS quicktake_100_load_raw()

```
....
2086.             + rstep[sharp][getbits(2)];
```

Buffer Overflow IndexFromInput\Path 48:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=102

Status	New

The size of the buffer used by quicktake_100_load_raw in getbits, at line 2036 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2065
Object	fgetc	getbits

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method void CLASS quicktake_100_load_raw()

```
....
2065.             pixel[row][col-2]) >> 2) + gstep[getbits(4)];
```

Buffer Overflow IndexFromInput\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=103
Status	New

The size of the buffer used by radc_token in getbits, at line 2120 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2157
Object	fgetc	getbits

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method int CLASS radc_token (int tree)

```
....
2157.      dindex = dindex->branch[getbits(1)];
```

Buffer Overflow IndexFromInput\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=104
Status	New

The size of the buffer used by kodak_radc_load_raw in c, at line 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2191
Object	fgetc	c

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method void CLASS kodak_radc_load_raw()

```
....
2191.            FORYX buf[c][y][x] = radc_token(tree+10) * mul[c];
```

Buffer Overflow LongString

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow LongString Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1
Status	New

The size of the buffer used by DetectAsn1TestReal01 in sigs, at line 1040 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal01 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 1040 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1091	1091
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal01(void)

```
....
1091.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\";
"
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=2
Status	New

The size of the buffer used by DetectAsn1TestReal01 in sigs, at line 1040 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal01 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 1040 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1094	1094
Object	"alert ip any any -> any any	sigs

	(msg:\"Testing id 2\"; "	

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal01(void)

```
....
1094.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\";
"
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3
Status	New

The size of the buffer used by DetectAsn1TestReal01 in sigs, at line 1040 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal01 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 1040 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1097	1097
Object	"alert ip any any -> any any (msg:\"Testing id 3\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal01(void)

```
....
1097.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\";
"
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4
Status	New

The size of the buffer used by DetectAsn1TestReal02 in sigs, at line 1119 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal02 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 1119 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1170	1170
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal02(void)

```
....
1170.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\";
"
```

Buffer Overflow LongString\Path 5:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=5
Status New

The size of the buffer used by DetectAsn1TestReal02 in sigs, at line 1119 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal02 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 1119 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1173	1173
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal02(void)

```
....
1173.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\";
"
```

Buffer Overflow LongString\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=6

Status	New

The size of the buffer used by DetectAsn1TestReal02 in sigs, at line 1119 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal02 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 1119 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1176	1176
Object	"alert ip any any -> any any (msg:\"Testing id 3\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal02(void)

```
....
1176.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\";
"
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=7
Status	New

The size of the buffer used by DetectAsn1TestReal03 in sigs, at line 1196 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal03 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 1196 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1230	1230
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal03(void)

```
....
1230.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\";
"
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=8
Status	New

The size of the buffer used by DetectAsn1TestReal03 in sigs, at line 1196 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal03 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 1196 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1233	1233
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet

File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c

Method static int DetectAsn1TestReal03(void)

```
....
1233.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\";
"
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=9
Status	New

The size of the buffer used by DetectAsn1TestReal03 in sigs, at line 1196 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal03 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 1196 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1237	1237
Object	"alert ip any any -> any any (msg:\"Testing id 3\"; "	sigs

Code Snippet

File Name	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method	static int DetectAsn1TestReal03(void)

```
....
1237.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\";
"
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=10
Status	New

The size of the buffer used by DetectAsn1TestReal04 in sigs, at line 1257 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal04 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 1257 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1308	1308
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet

File Name	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method	static int DetectAsn1TestReal04(void)

```
....
1308.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\";
"
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=11
Status	New

The size of the buffer used by DetectAsn1TestReal04 in sigs, at line 1257 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal04 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 1257 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-	OISF@@suricata-suricata-5.0.2-CVE-

	2023-35853-TP.c	2023-35853-TP.c
Line	1311	1311
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal04(void)

```
....
1311.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\";
"
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=12
Status	New

The size of the buffer used by DetectAsn1TestReal04 in sigs, at line 1257 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal04 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 1257 of OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	1314	1314
Object	"alert ip any any -> any any (msg:\"Testing id 3\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal04(void)

```
....
1314.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\";
"
```

Buffer Overflow LongString\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=13
Status	New

The size of the buffer used by DetectAsn1TestReal01 in sigs, at line 173 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal01 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 173 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	224	224
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal01(void)

```
....
224.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\"; "
```

Buffer Overflow LongString\Path 14:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=14
Status New

The size of the buffer used by DetectAsn1TestReal01 in sigs, at line 173 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal01 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 173 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	227	227
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal01(void)

```
....
227.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\"; "
```

Buffer Overflow LongString\Path 15:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=15
Status	New

The size of the buffer used by DetectAsn1TestReal01 in sigs, at line 173 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal01 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 173 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	230	230
Object	"alert ip any any -> any any (msg:\"Testing id 3\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal01(void)

```
....
230.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\"; "
```

Buffer Overflow LongString\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=16
Status	New

The size of the buffer used by DetectAsn1TestReal02 in sigs, at line 252 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal02 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 252 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	303	303
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal02(void)

```
....
303.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\"; "
```

Buffer Overflow LongString\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=17
Status	New

The size of the buffer used by DetectAsn1TestReal02 in sigs, at line 252 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal02 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 252 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	306	306
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal02(void)

```
....
306.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\"; "
```

Buffer Overflow LongString\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=18
Status	New

The size of the buffer used by DetectAsn1TestReal02 in sigs, at line 252 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal02 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 252 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	309	309
Object	"alert ip any any -> any any	sigs

	(msg:\"Testing id 3\"; "	

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal02(void)

```
....
309.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\"; "
```

Buffer Overflow LongString\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=19
Status	New

The size of the buffer used by DetectAsn1TestReal03 in sigs, at line 329 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal03 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 329 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	363	363
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal03(void)

```
....
363.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\"; "
```

Buffer Overflow LongString\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=20
Status	New

The size of the buffer used by DetectAsn1TestReal03 in sigs, at line 329 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal03 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 329 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination

File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	366	366
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal03(void)

```
....
366.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\"; "
```

Buffer Overflow LongString\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=21
Status	New

The size of the buffer used by DetectAsn1TestReal03 in sigs, at line 329 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal03 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 329 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	370	370
Object	"alert ip any any -> any any (msg:\"Testing id 3\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal03(void)

```
....
370.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\"; "
```

Buffer Overflow LongString\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=22
Status	New

The size of the buffer used by DetectAsn1TestReal04 in sigs, at line 390 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal04 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 390 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	441	441
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal04(void)

```
....
441.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\"; "
```

Buffer Overflow LongString\Path 23:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=23
Status New

The size of the buffer used by DetectAsn1TestReal04 in sigs, at line 390 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal04 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 390 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	444	444
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal04(void)

```
....
444.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\"; "
```

Buffer Overflow LongString\Path 24:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=24
Status	New

The size of the buffer used by DetectAsn1TestReal04 in sigs, at line 390 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal04 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 390 of OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Line	447	447
Object	"alert ip any any -> any any (msg:\"Testing id 3\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.12-CVE-2023-35853-TP.c
Method static int DetectAsn1TestReal04(void)

```
....
447.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\"; "
```

Buffer Overflow LongString\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=25
Status	New

The size of the buffer used by DetectAsn1TestReal01 in sigs, at line 173 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal01 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 173 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	224	224
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method static int DetectAsn1TestReal01(void)

```
....
224.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\"; "
```

Buffer Overflow LongString\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=26
Status	New

The size of the buffer used by DetectAsn1TestReal01 in sigs, at line 173 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal01 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 173 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	227	227
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet

File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c

Method static int DetectAsn1TestReal01(void)

```
....
227.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\"; "
```

Buffer Overflow LongString\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=27
Status	New

The size of the buffer used by DetectAsn1TestReal01 in sigs, at line 173 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal01 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 173 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	230	230
Object	"alert ip any any -> any any	sigs

	(msg:\"Testing id 3\"; "	

Code Snippet
File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method static int DetectAsn1TestReal01(void)

```
....
230.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\"; "
```

Buffer Overflow LongString\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=28
Status	New

The size of the buffer used by DetectAsn1TestReal02 in sigs, at line 252 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal02 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 252 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	303	303
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method static int DetectAsn1TestReal02(void)

```
....
303.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\"; "
```

Buffer Overflow LongString\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=29
Status	New

The size of the buffer used by DetectAsn1TestReal02 in sigs, at line 252 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal02 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 252 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination

File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	306	306
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method static int DetectAsn1TestReal02(void)

```
....
306.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\"; "
```

Buffer Overflow LongString\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=30
Status	New

The size of the buffer used by DetectAsn1TestReal02 in sigs, at line 252 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal02 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 252 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	309	309
Object	"alert ip any any -> any any (msg:\"Testing id 3\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method static int DetectAsn1TestReal02(void)

```
....
309.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\"; "
```

Buffer Overflow LongString\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=31
Status	New

The size of the buffer used by DetectAsn1TestReal03 in sigs, at line 329 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal03 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 329 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	363	363
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method static int DetectAsn1TestReal03(void)

```
....
363.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\"; "
```

Buffer Overflow LongString\Path 32:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=32
Status New

The size of the buffer used by DetectAsn1TestReal03 in sigs, at line 329 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal03 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 329 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	366	366
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method static int DetectAsn1TestReal03(void)

```
....
366.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\"; "
```

Buffer Overflow LongString\Path 33:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=33
Status	New

The size of the buffer used by DetectAsn1TestReal03 in sigs, at line 329 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal03 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 329 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	370	370
Object	"alert ip any any -> any any (msg:\"Testing id 3\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method static int DetectAsn1TestReal03(void)

```
....
370.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\"; "
```

Buffer Overflow LongString\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=34
Status	New

The size of the buffer used by DetectAsn1TestReal04 in sigs, at line 390 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal04 passes to "alert ip any any -> any any (msg:\"Testing id 1\"; ", at line 390 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	441	441
Object	"alert ip any any -> any any (msg:\"Testing id 1\"; "	sigs

Code Snippet
File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method static int DetectAsn1TestReal04(void)

```
....
441.      sigs[0]= "alert ip any any -> any any (msg:\"Testing id 1\"; "
```

Buffer Overflow LongString\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=35
Status	New

The size of the buffer used by DetectAsn1TestReal04 in sigs, at line 390 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal04 passes to "alert ip any any -> any any (msg:\"Testing id 2\"; ", at line 390 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	444	444
Object	"alert ip any any -> any any (msg:\"Testing id 2\"; "	sigs

Code Snippet

File Name	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method	static int DetectAsn1TestReal04(void)

```
....
444.      sigs[1]= "alert ip any any -> any any (msg:\"Testing id 2\"; "
```

Buffer Overflow LongString\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=36
Status	New

The size of the buffer used by DetectAsn1TestReal04 in sigs, at line 390 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that DetectAsn1TestReal04 passes to "alert ip any any -> any any (msg:\"Testing id 3\"; ", at line 390 of OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Line	447	447
Object	"alert ip any any -> any any	sigs

	(msg:\"Testing id 3\"; "	

Code Snippet
File Name OISF@@suricata-suricata-6.0.14-CVE-2023-35853-FP.c
Method static int DetectAsn1TestReal04(void)

```
....
447.      sigs[2]= "alert ip any any -> any any (msg:\"Testing id 3\"; "
```

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=1020047&projectid=20040&pathid=37
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4831	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20

	040&pathid=38
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4842	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=39
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4846	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=40
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4848	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=41
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4851	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=42
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4855	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=43
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4831	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=44
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4842	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=45
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-	ONLYOFFICE@@core-v5.5.2.2-CVE-

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

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=46
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4848	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=47
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4851	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=48
Status	New

The size of the buffer used by parse_mos in flip, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4855	4867
Object	ifp	flip

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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];
```

CGI Stored XSS

Query Path:
CPP\Cx\CPP High Risk\CGI Stored XSS Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)

Description

CGI Stored XSS\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=392
Status	New

Unvalidated DB output was found in line number 1369 in ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c file. A possible XSS exploitation was found in putc at line number 1369.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1380	1382
Object	thumb	putc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS layer_thumb (FILE *tfp)

```
....
1380.    fread (thumb, thumb_length, colors, ifp);
....
1382.      FORCC putc (thumb[i+thumb_length*(map[thumb_misc >> 8][c]-
'0')], tfp);
```

CGI Stored XSS\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=393
Status	New

Unvalidated DB output was found in line number 342 in ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c file. A possible XSS exploitation was found in putc at line number 1386.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	344	1397
Object	pixel	putc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c

Method void CLASS rollei_thumb (FILE *tfp)

```
....
1397.       putc (thumb[i] << 3, tfp);
```

CGI Stored XSS\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=394
Status	New

Unvalidated DB output was found in line number 342 in ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c file. A possible XSS exploitation was found in putc at line number 1386.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	344	1398
Object	pixel	putc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c

Method void CLASS rollei_thumb (FILE *tfp)

```
....
1398.       putc (thumb[i] >> 5  << 2, tfp);
```

CGI Stored XSS\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=395
Status	New

Unvalidated DB output was found in line number 342 in ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c file. A possible XSS exploitation was found in putc at line number 1386.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	344	1399
Object	pixel	putc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS rollei_thumb (FILE *tfp)

```
....
1399.       putc (thumb[i] >> 11 << 3, tfp);
```

CGI Stored XSS\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=396
Status	New

Unvalidated DB output was found in line number 1369 in ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c file. A possible XSS exploitation was found in putc at line number 1369.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	1380	1382
Object	thumb	putc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS layer_thumb (FILE *tfp)

```
....
1380.    fread (thumb, thumb_length, colors, ifp);
....
1382.      FORCC putc (thumb[i+thumb_length*(map[thumb_misc >> 8][c]-
'0')], tfp);
```

CGI Stored XSS\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=397
Status	New

Unvalidated DB output was found in line number 342 in ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c file. A possible XSS exploitation was found in putc at line number 1386.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	344	1397
Object	pixel	putc

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c

Method void CLASS rollei_thumb (FILE *tfp)

```
....
1397.      putc (thumb[i] << 3, tfp);
```

CGI Stored XSS\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=398
Status	New

Unvalidated DB output was found in line number 342 in ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c file. A possible XSS exploitation was found in putc at line number 1386.

	Source	Destination

File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	344	1398
Object	pixel	putc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS rollei_thumb (FILE *tfp)

```
....
1398.       putc (thumb[i] >> 5  << 2, tfp);
```

CGI Stored XSS\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=399
Status	New

Unvalidated DB output was found in line number 342 in ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c file. A possible XSS exploitation was found in putc at line number 1386.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	344	1399
Object	pixel	putc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS rollei_thumb (FILE *tfp)

```
....
1399.       putc (thumb[i] >> 11 << 3, tfp);
```

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=1020047&projectid=20040&pathid=49
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=50
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=51
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20

	040&pathid=52
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=53
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=54
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=382
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-	ONLYOFFICE@@core-v5.4.99.1786-CVE-

	2022-29776-FP.c	2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=383
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=384
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=385
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20

	040&pathid=386
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=387
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=380
Status	New

Method parse_riff at line 5849 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c at line 5849.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-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=1020047&projectid=20040&pathid=381
Status	New

Method parse_riff at line 5849 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c at line 5849.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-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=1020047&projectid=20040&pathid=1586
Status	New

The dangerous function, _snprintf, was found in use at line 8313 in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8655	8655
Object	_snprintf	_snprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1587
Status	New

The dangerous function, _snprintf, was found in use at line 8313 in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8655	8655
Object	_snprintf	_snprintf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1588
Status New

The dangerous function, _tcslen, was found in use at line 3323 in notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	3392	3392
Object	_tcslen	_tcslen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3392.                                 if (_tcslen(kwl) < max_char)
```

Dangerous Functions\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1589
Status New

The dangerous function, _tcslen, was found in use at line 3343 in notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	3412	3412
Object	_tcslen	_tcslen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3412.                                   if (_tcslen(kwl) < max_char)
```

Dangerous Functions\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1590
Status New

The dangerous function, _tcslen, was found in use at line 3366 in notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	3435	3435
Object	_tcslen	_tcslen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3435.                                   if (_tcslen(kwl) < max_char)
```

Dangerous Functions\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1591

Status	New

The dangerous function, _tcslen, was found in use at line 3406 in notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	3475	3475
Object	_tcslen	_tcslen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3475.                                   if (_tcslen(kwl) < max_char)
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1592
Status	New

The dangerous function, _tcslen, was found in use at line 3435 in notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	3504	3504
Object	_tcslen	_tcslen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3504.                                   if (_tcslen(kwl) < max_char)
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=1593
Status	New

The dangerous function, _tcslen, was found in use at line 3456 in notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Line	3525	3525
Object	_tcslen	_tcslen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3525.                                   if (_tcslen(kwl) < max_char)
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1594
Status	New

The dangerous function, _tcslen, was found in use at line 3496 in notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Line	3565	3565
Object	_tcslen	_tcslen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3565.                                   if (_tcslen(kwl) < max_char)
```

Dangerous Functions\Path 10:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1595
Status	New

The dangerous function, _tcslen, was found in use at line 3551 in notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	3620	3620
Object	_tcslen	_tcslen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3620.                                   if (_tcslen(kwl) < max_char)
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1596
Status	New

The dangerous function, _tcslen, was found in use at line 3553 in notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c
Line	3622	3622
Object	_tcslen	_tcslen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3622.                                   if (_tcslen(kwl) < max_char)
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1597
Status	New

The dangerous function, _ui64tot, was found in use at line 3290 in notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	3363	3363
Object	_ui64tot	_ui64tot

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method void NppParameters::writeSession(const Session & session, const TCHAR *fileName)

```
....
3363.                                   markNode->ToElement()-
>SetAttribute(TEXT("line"), _ui64tot(static_cast<ULONGLONG>(markLine),
szInt64, 10));
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1598
Status	New

The dangerous function, _ui64tot, was found in use at line 3290 in notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	3370	3370
Object	_ui64tot	_ui64tot

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method void NppParameters::writeSession(const Session & session, const TCHAR *fileName)

```
....
3370.                                   foldNode->ToElement()-
>SetAttribute(TEXT("line"), _ui64tot(static_cast<ULONGLONG>(foldLine),
szInt64, 10));
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1599
Status	New

The dangerous function, _ui64tot, was found in use at line 3292 in notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c
Line	3365	3365
Object	_ui64tot	_ui64tot

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c
Method void NppParameters::writeSession(const Session & session, const TCHAR *fileName)

```
....
3365.                                   markNode->ToElement()-
>SetAttribute(TEXT("line"), _ui64tot(static_cast<ULONGLONG>(markLine),
szInt64, 10));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1600
Status	New

The dangerous function, _ui64tot, was found in use at line 3292 in notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c
Line	3372	3372

Object	_ui64tot	_ui64tot

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c
Method void NppParameters::writeSession(const Session & session, const TCHAR *fileName)

```
....
3372.                                   foldNode->ToElement()-
>SetAttribute(TEXT("line"), _ui64tot(static_cast<ULONGLONG>(foldLine),
szInt64, 10));
```

Dangerous Functions\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1601
Status New

The dangerous function, lstrcpyn, was found in use at line 3990 in notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	4999	4999
Object	lstrcpyn	lstrcpyn

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method void NppParameters::feedGUIParameters(TiXmlNode *node)

```
....
4999.                           lstrcpyn(_nppGUI._defaultDir, path,
MAX_PATH);
```

Dangerous Functions\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1602
Status New

The dangerous function, lstrcpyn, was found in use at line 4012 in notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	5054	5054
Object	lstrcpyn	lstrcpyn

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::feedGUIParameters(TiXmlNode *node)

```
....
5054.                           lstrcpyn(_nppGUI._defaultDir, path,
MAX_PATH);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1603
Status	New

The dangerous function, lstrcpyn, was found in use at line 4047 in notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	5105	5105
Object	lstrcpyn	lstrcpyn

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::feedGUIParameters(TiXmlNode *node)

```
....
5105.                           lstrcpyn(_nppGUI._defaultDir, path,
MAX_PATH);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1604
Status	New

The dangerous function, lstrcpyn, was found in use at line 4091 in notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	5160	5160
Object	lstrcpyn	lstrcpyn

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::feedGUIParameters(TiXmlNode *node)

```
....
5160.                           lstrcpyn(_nppGUI._defaultDir, path,
MAX_PATH);
```

Dangerous Functions\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1605
Status New

The dangerous function, lstrcpyn, was found in use at line 4120 in notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	5219	5219
Object	lstrcpyn	lstrcpyn

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::feedGUIParameters(TiXmlNode *node)

```
....
5219.                           lstrcpyn(_nppGUI._defaultDir, path,
MAX_PATH);
```

Dangerous Functions\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=1606
Status	New

The dangerous function, lstrcpyn, was found in use at line 4126 in notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Line	5248	5248
Object	lstrcpyn	lstrcpyn

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Method void NppParameters::feedGUIParameters(TiXmlNode *node)

```
....
5248.                           lstrcpyn(_nppGUI._defaultDir, path,
MAX_PATH);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1607
Status	New

The dangerous function, lstrcpyn, was found in use at line 4166 in notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Line	5297	5297
Object	lstrcpyn	lstrcpyn

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Method void NppParameters::feedGUIParameters(TiXmlNode *node)

```
....
5297.                           lstrcpyn(_nppGUI._defaultDir, path,
MAX_PATH);
```

Dangerous Functions\Path 23:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1608
Status	New

The dangerous function, lstrcpyn, was found in use at line 4223 in notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	5354	5354
Object	lstrcpyn	lstrcpyn

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method void NppParameters::feedGUIParameters(TiXmlNode *node)

```
....
5354.                           lstrcpyn(_nppGUI._defaultDir, path,
MAX_PATH);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1609
Status	New

The dangerous function, lstrcpyn, was found in use at line 4237 in notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c
Line	5379	5379
Object	lstrcpyn	lstrcpyn

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c
Method void NppParameters::feedGUIParameters(TiXmlNode *node)

```
....
5379.                           lstrcpyn(_nppGUI._defaultDir, path,
MAX_PATH);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1610
Status	New

The dangerous function, lstrlen, was found in use at line 2469 in notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	2493	2493
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method void NppParameters::feedPluginCustomizedCmds(TiXmlNode *node)

```
....
2493.                    if (!generic_strnicmp(pscOrig.getModuleName(),
moduleName, lstrlen(moduleName)) && pscOrig.getInternalID() ==
internalID)
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1611
Status	New

The dangerous function, lstrlen, was found in use at line 6682 in notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	6692	6692
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6692.                          const size_t strLen =
lstrlen(style._styleDesc) + 1;
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1612
Status	New

The dangerous function, lstrlen, was found in use at line 6682 in notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	6698	6698
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6698.                                  const size_t strLen2 =
lstrlen(style._fontName) + 1;
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1613
Status	New

The dangerous function, lstrlen, was found in use at line 6868 in notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	6872	6872
Object	lstrlen	lstrlen

Code Snippet	
File Name	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method	Date::Date(const TCHAR *dateStr)

```
....
6872.       int D = lstrlen(dateStr);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1614
Status	New

The dangerous function, lstrlen, was found in use at line 2489 in notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	2513	2513
Object	lstrlen	lstrlen

Code Snippet	
File Name	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method	void NppParameters::feedPluginCustomizedCmds(TiXmlNode *node)

```
....
2513.                   if (!generic_strnicmp(pscOrig.getModuleName(),
moduleName, lstrlen(moduleName)) && pscOrig.getInternalID() ==
internalID)
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1615
Status	New

The dangerous function, lstrlen, was found in use at line 6746 in notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	6756	6756

Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6756.                         const size_t strLen =
lstrlen(style._styleDesc) + 1;
```

Dangerous Functions\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1616
Status New

The dangerous function, lstrlen, was found in use at line 6746 in notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	6762	6762
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6762.                                 const size_t strLen2 =
lstrlen(style._fontName) + 1;
```

Dangerous Functions\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1617
Status New

The dangerous function, lstrlen, was found in use at line 6932 in notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-	notepad-plus-plus@@notepad-plus-plus-

	v7.8.7-CVE-2022-32168-FP.c	v7.8.7-CVE-2022-32168-FP.c
Line	6936	6936
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method Date::Date(const TCHAR *dateStr)

```
....
6936.       int D = lstrlen(dateStr);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1618
Status	New

The dangerous function, lstrlen, was found in use at line 2512 in notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	2536	2536
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::feedPluginCustomizedCmds(TiXmlNode *node)

```
....
2536.                   if (!generic_strnicmp(pscOrig.getModuleName(),
moduleName, lstrlen(moduleName)) && pscOrig.getInternalID() ==
internalID)
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1619
Status	New

The dangerous function, lstrlen, was found in use at line 6843 in notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	6853	6853
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6853.                          const size_t strLen =
lstrlen(style._styleDesc) + 1;
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1620
Status	New

The dangerous function, lstrlen, was found in use at line 6843 in notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	6859	6859
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6859.                                  const size_t strLen2 =
lstrlen(style._fontName) + 1;
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1621
Status	New

The dangerous function, lstrlen, was found in use at line 7029 in notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	7033	7033
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method Date::Date(const TCHAR *dateStr)

```
....
7033.       int D = lstrlen(dateStr);
```

Dangerous Functions\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1622
Status New

The dangerous function, lstrlen, was found in use at line 2529 in notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	2553	2553
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::feedPluginCustomizedCmds(TiXmlNode *node)

```
....
2553.                   if (!generic_strnicmp(pscOrig.getModuleName(),
moduleName, lstrlen(moduleName)) && pscOrig.getInternalID() ==
internalID)
```

Dangerous Functions\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=1623
Status	New

The dangerous function, lstrlen, was found in use at line 7053 in notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	7063	7063
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
7063.                          const size_t strLen =
lstrlen(style._styleDesc) + 1;
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1624
Status	New

The dangerous function, lstrlen, was found in use at line 7053 in notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	7069	7069
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
7069.                                  const size_t strLen2 =
lstrlen(style._fontName) + 1;
```

Dangerous Functions\Path 40:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1625
Status	New

The dangerous function, lstrlen, was found in use at line 7239 in notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	7243	7243
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method Date::Date(const TCHAR *dateStr)

```
....
7243.       int D = lstrlen(dateStr);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1626
Status	New

The dangerous function, lstrlen, was found in use at line 2558 in notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	2582	2582
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::feedPluginCustomizedCmds(TiXmlNode *node)

```
....
2582.                   if (!generic_strnicmp(pscOrig.getModuleName(),
moduleName, lstrlen(moduleName)) && pscOrig.getInternalID() ==
internalID)
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1627
Status	New

The dangerous function, lstrlen, was found in use at line 7214 in notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	7224	7224
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
7224.                          const size_t strLen =
lstrlen(style._styleDesc) + 1;
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1628
Status	New

The dangerous function, lstrlen, was found in use at line 7214 in notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	7230	7230
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
7230.                                   const size_t strLen2 =
lstrlen(style._fontName) + 1;
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1629
Status	New

The dangerous function, lstrlen, was found in use at line 7400 in notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	7404	7404
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method Date::Date(const TCHAR *dateStr)

```
....
7404.       int D = lstrlen(dateStr);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1630
Status	New

The dangerous function, lstrlen, was found in use at line 2577 in notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Line	2601	2601
Object	lstrlen	lstrlen

Code Snippet

File Name	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Method	void NppParameters::feedPluginCustomizedCmds(TiXmlNode *node)

```
....
2601.                    if (!generic_strnicmp(pscOrig.getModuleName(),
moduleName, lstrlen(moduleName)) && pscOrig.getInternalID() ==
internalID)
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1631
Status	New

The dangerous function, lstrlen, was found in use at line 7482 in notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Line	7486	7486
Object	lstrlen	lstrlen

Code Snippet	
File Name	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Method	Date::Date(const TCHAR *dateStr)

```
....
7486.       int D = lstrlen(dateStr);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1632
Status	New

The dangerous function, lstrlen, was found in use at line 2617 in notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Line	2641	2641

Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Method void NppParameters::feedPluginCustomizedCmds(TiXmlNode *node)

```
....
2641.                   if (!generic_strnicmp(pscOrig.getModuleName(),
moduleName, lstrlen(moduleName)) && pscOrig.getInternalID() ==
internalID)
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1633
Status	New

The dangerous function, lstrlen, was found in use at line 7537 in notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Line	7541	7541
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Method Date::Date(const TCHAR *dateStr)

```
....
7541.       int D = lstrlen(dateStr);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1634
Status	New

The dangerous function, lstrlen, was found in use at line 2670 in notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-	notepad-plus-plus@@notepad-plus-plus-

	v8.4.1-CVE-2022-32168-TP.c	v8.4.1-CVE-2022-32168-TP.c
Line	2694	2694
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method void NppParameters::feedPluginCustomizedCmds(TiXmlNode *node)

```
....
2694.                    if (!generic_strnicmp(pscOrig.getModuleName(),
moduleName, lstrlen(moduleName)) && pscOrig.getInternalID() ==
internalID)
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1635
Status	New

The dangerous function, lstrlen, was found in use at line 7647 in notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	7651	7651
Object	lstrlen	lstrlen

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method Date::Date(const TCHAR *dateStr)

```
....
7651.       int D = lstrlen(dateStr);
```

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=1020047&projectid=20040&pathid=400
Status	New

The size of the buffer used by ac_match_handler in AC_REP_t, at line 1796 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ac_match_handler passes to AC_REP_t, at line 1796 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	1836	1836
Object	AC_REP_t	AC_REP_t

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method static int ac_match_handler(AC_MATCH_t *m, AC_TEXT_t *txt, AC_REP_t *match) {

```
....
1836.       memcpy(match, &m->patterns[0].rep, sizeof(AC_REP_t)); /*
Partial match? */
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=401
Status	New

The size of the buffer used by ac_match_handler in AC_REP_t, at line 1796 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ac_match_handler passes to AC_REP_t, at line 1796 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	1847	1847
Object	AC_REP_t	AC_REP_t

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method static int ac_match_handler(AC_MATCH_t *m, AC_TEXT_t *txt, AC_REP_t *match) {

```
....
1847.    memcpy(match, &m->patterns[0].rep, sizeof(AC_REP_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=402
Status	New

The size of the buffer used by ndpi_set_protocol_detection_bitmask2 in ndpi_call_function_struct, at line 3033 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ndpi_set_protocol_detection_bitmask2 passes to ndpi_call_function_struct, at line 3033 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3545	3545
Object	ndpi_call_function_struct	ndpi_call_function_struct

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method void ndpi_set_protocol_detection_bitmask2(struct ndpi_detection_module_struct *ndpi_str,

```
....
3545.             &ndpi_str->callback_buffer[a], sizeof(struct
ndpi_call_function_struct));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=403
Status	New

The size of the buffer used by ndpi_set_protocol_detection_bitmask2 in ndpi_call_function_struct, at line 3033 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ndpi_set_protocol_detection_bitmask2 passes to ndpi_call_function_struct, at line 3033 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3555	3555
Object	ndpi_call_function_struct	ndpi_call_function_struct

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method void ndpi_set_protocol_detection_bitmask2(struct ndpi_detection_module_struct *ndpi_str,

```
....
3555.              sizeof(struct ndpi_call_function_struct));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=404
Status	New

The size of the buffer used by ndpi_set_protocol_detection_bitmask2 in ndpi_call_function_struct, at line 3033 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ndpi_set_protocol_detection_bitmask2 passes to ndpi_call_function_struct, at line 3033 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3571	3571
Object	ndpi_call_function_struct	ndpi_call_function_struct

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method void ndpi_set_protocol_detection_bitmask2(struct ndpi_detection_module_struct *ndpi_str,

```
....
3571.              &ndpi_str->callback_buffer[a], sizeof(struct
ndpi_call_function_struct));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=405
Status	New

The size of the buffer used by ndpi_set_protocol_detection_bitmask2 in ndpi_call_function_struct, at line 3033 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ndpi_set_protocol_detection_bitmask2 passes to ndpi_call_function_struct, at line 3033 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3587	3587
Object	ndpi_call_function_struct	ndpi_call_function_struct

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method void ndpi_set_protocol_detection_bitmask2(struct ndpi_detection_module_struct *ndpi_str,

```
....
3587.             &ndpi_str->callback_buffer[a], sizeof(struct
ndpi_call_function_struct));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=406
Status New

The size of the buffer used by ndpi_apply_flow_protocol_to_packet in ->, at line 3744 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ndpi_apply_flow_protocol_to_packet passes to ->, at line 3744 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3747	3747
Object	->	->

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method void ndpi_apply_flow_protocol_to_packet(struct ndpi_flow_struct *flow,

```
....
3747.    memcpy(&packet->detected_protocol_stack, &flow-
>detected_protocol_stack, sizeof(packet->detected_protocol_stack));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=407
Status New

The size of the buffer used by ndpi_apply_flow_protocol_to_packet in ->, at line 3744 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ndpi_apply_flow_protocol_to_packet passes to ->, at line 3744 of ntop@@nDPI-3.2-CVE-2020-15475-TP.c, to overwrite the target buffer.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3748	3748

Object	->	->

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method void ndpi_apply_flow_protocol_to_packet(struct ndpi_flow_struct *flow,

```
....
3748.    memcpy(&packet->protocol_stack_info, &flow-
>protocol_stack_info, sizeof(packet->protocol_stack_info));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=408
Status	New

The size of the buffer used by ndpi_search_netbios in netbios_header, at line 99 of ntop@@nDPI-3.4-CVE-2021-36082-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ndpi_search_netbios passes to netbios_header, at line 99 of ntop@@nDPI-3.4-CVE-2021-36082-TP.c, to overwrite the target buffer.

	Source	Destination
File	ntop@@nDPI-3.4-CVE-2021-36082-TP.c	ntop@@nDPI-3.4-CVE-2021-36082-TP.c
Line	113	113
Object	netbios_header	netbios_header

Code Snippet
File Name ntop@@nDPI-3.4-CVE-2021-36082-TP.c
Method void ndpi_search_netbios(struct ndpi_detection_module_struct *ndpi_struct,

```
....
113.        memcpy(&h, packet->payload, sizeof(struct netbios_header));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=409
Status	New

The size of the buffer used by *caf_open in pcm_io_context_t, at line 216 of nu774@@fdkaac-v1.0.1-CVE-2022-36148-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *caf_open passes to pcm_io_context_t, at line 216 of nu774@@fdkaac-v1.0.1-CVE-2022-36148-TP.c, to overwrite the target buffer.

	Source	Destination
File	nu774@@fdkaac-v1.0.1-CVE-2022-36148-TP.c	nu774@@fdkaac-v1.0.1-CVE-2022-36148-TP.c

Line	225	225
Object	pcm_io_context_t	pcm_io_context_t

Code Snippet
File Name nu774@@fdkaac-v1.0.1-CVE-2022-36148-TP.c
Method pcm_reader_t *caf_open(pcm_io_context_t *io,

```
....
225.      memcpy(&reader->io, io, sizeof(pcm_io_context_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=410
Status	New

The size of the buffer used by *caf_open in pcm_io_context_t, at line 216 of nu774@@fdkaac-v1.0.1-CVE-2023-34823-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *caf_open passes to pcm_io_context_t, at line 216 of nu774@@fdkaac-v1.0.1-CVE-2023-34823-TP.c, to overwrite the target buffer.

	Source	Destination
File	nu774@@fdkaac-v1.0.1-CVE-2023-34823-TP.c	nu774@@fdkaac-v1.0.1-CVE-2023-34823-TP.c
Line	225	225
Object	pcm_io_context_t	pcm_io_context_t

Code Snippet
File Name nu774@@fdkaac-v1.0.1-CVE-2023-34823-TP.c
Method pcm_reader_t *caf_open(pcm_io_context_t *io,

```
....
225.      memcpy(&reader->io, io, sizeof(pcm_io_context_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=411
Status	New

The size of the buffer used by *caf_open in pcm_io_context_t, at line 216 of nu774@@fdkaac-v1.0.2-CVE-2022-36148-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *caf_open passes to pcm_io_context_t, at line 216 of nu774@@fdkaac-v1.0.2-CVE-2022-36148-TP.c, to overwrite the target buffer.

	Source	Destination
File	nu774@@fdkaac-v1.0.2-CVE-2022-	nu774@@fdkaac-v1.0.2-CVE-2022-

	36148-TP.c	36148-TP.c
Line	225	225
Object	pcm_io_context_t	pcm_io_context_t

Code Snippet
File Name nu774@@fdkaac-v1.0.2-CVE-2022-36148-TP.c
Method pcm_reader_t *caf_open(pcm_io_context_t *io,

```
....
225.      memcpy(&reader->io, io, sizeof(pcm_io_context_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=412
Status	New

The size of the buffer used by *caf_open in pcm_io_context_t, at line 216 of nu774@@fdkaac-v1.0.2-CVE-2023-34823-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *caf_open passes to pcm_io_context_t, at line 216 of nu774@@fdkaac-v1.0.2-CVE-2023-34823-TP.c, to overwrite the target buffer.

	Source	Destination
File	nu774@@fdkaac-v1.0.2-CVE-2023-34823-TP.c	nu774@@fdkaac-v1.0.2-CVE-2023-34823-TP.c
Line	225	225
Object	pcm_io_context_t	pcm_io_context_t

Code Snippet
File Name nu774@@fdkaac-v1.0.2-CVE-2023-34823-TP.c
Method pcm_reader_t *caf_open(pcm_io_context_t *io,

```
....
225.      memcpy(&reader->io, io, sizeof(pcm_io_context_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=413
Status	New

The size of the buffer used by *caf_open in pcm_io_context_t, at line 218 of nu774@@fdkaac-v1.0.3-CVE-2023-34823-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *caf_open passes to pcm_io_context_t, at line 218 of nu774@@fdkaac-v1.0.3-CVE-2023-34823-TP.c, to overwrite the target buffer.

	Source	Destination

File	nu774@@fdkaac-v1.0.3-CVE-2023-34823-TP.c	nu774@@fdkaac-v1.0.3-CVE-2023-34823-TP.c
Line	227	227
Object	pcm_io_context_t	pcm_io_context_t

Code Snippet
File Name nu774@@fdkaac-v1.0.3-CVE-2023-34823-TP.c
Method pcm_reader_t *caf_open(pcm_io_context_t *io,

```
....
227.      memcpy(&reader->io, io, sizeof(pcm_io_context_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=414
Status New

The size of the buffer used by htp_connp_res_data in timestamp, at line 1194 of OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that htp_connp_res_data passes to timestamp, at line 1194 of OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c
Line	1243	1243
Object	timestamp	timestamp

Code Snippet
File Name OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c
Method int htp_connp_res_data(htp_connp_t *connp, const htp_time_t *timestamp, const void *data, size_t len) {

```
....
1243.          memcpy(&connp->out_timestamp, timestamp, sizeof
(*timestamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=415
Status New

The size of the buffer used by htp_connp_res_data in timestamp, at line 1207 of OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that htp_connp_res_data passes to timestamp, at line 1207 of OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c
Line	1256	1256
Object	timestamp	timestamp

Code Snippet
File Name OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c
Method int htp_connp_res_data(htp_connp_t *connp, const htp_time_t *timestamp, const void *data, size_t len) {

```
....
1256.          memcpy(&connp->out_timestamp, timestamp, sizeof
(*timestamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=416
Status New

The size of the buffer used by htp_connp_res_data in timestamp, at line 1225 of OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that htp_connp_res_data passes to timestamp, at line 1225 of OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c
Line	1274	1274
Object	timestamp	timestamp

Code Snippet
File Name OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c
Method int htp_connp_res_data(htp_connp_t *connp, const htp_time_t *timestamp, const void *data, size_t len) {

```
....
1274.          memcpy(&connp->out_timestamp, timestamp, sizeof
(*timestamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=417
Status	New

The size of the buffer used by htp_connp_res_data in timestamp, at line 1227 of OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that htp_connp_res_data passes to timestamp, at line 1227 of OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c
Line	1276	1276
Object	timestamp	timestamp

Code Snippet
File Name OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c
Method int htp_connp_res_data(htp_connp_t *connp, const htp_time_t *timestamp, const void *data, size_t len) {

```
....
1276.           memcpy(&connp->out_timestamp, timestamp, sizeof
(*timestamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=418
Status	New

The size of the buffer used by htp_connp_res_data in timestamp, at line 1227 of OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that htp_connp_res_data passes to timestamp, at line 1227 of OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c
Line	1276	1276
Object	timestamp	timestamp

Code Snippet
File Name OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c
Method int htp_connp_res_data(htp_connp_t *connp, const htp_time_t *timestamp, const void *data, size_t len) {

```
....
1276.           memcpy(&connp->out_timestamp, timestamp, sizeof
(*timestamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=419
Status	New

The size of the buffer used by htp_connp_res_data in timestamp, at line 1235 of OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that htp_connp_res_data passes to timestamp, at line 1235 of OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c
Line	1284	1284
Object	timestamp	timestamp

Code Snippet

File Name OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c

Method int htp_connp_res_data(htp_connp_t *connp, const htp_time_t *timestamp, const void *data, size_t len) {

```
....
1284.           memcpy(&connp->out_timestamp, timestamp, sizeof
(*timestamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=420
Status	New

The size of the buffer used by htp_connp_req_data in timestamp, at line 967 of OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that htp_connp_req_data passes to timestamp, at line 967 of OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c
Line	1015	1015
Object	timestamp	timestamp

Code Snippet

File Name OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c

Method int htp_connp_req_data(htp_connp_t *connp, const htp_time_t *timestamp, const void *data, size_t len) {

```
....
1015.          memcpy(&connp->in_timestamp, timestamp, sizeof
(*timestamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=421
Status	New

The size of the buffer used by htp_connp_req_data in timestamp, at line 967 of OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that htp_connp_req_data passes to timestamp, at line 967 of OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c
Line	1015	1015
Object	timestamp	timestamp

Code Snippet
File Name OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c
Method int htp_connp_req_data(htp_connp_t *connp, const htp_time_t *timestamp, const void *data, size_t len) {

```
....
1015.          memcpy(&connp->in_timestamp, timestamp, sizeof
(*timestamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=422
Status	New

The size of the buffer used by AddressTestIPv6Le05 in Namespace538243107, at line 985 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6Le05 passes to Namespace538243107, at line 985 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	995	995

Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6Le05(void)

```
....
995.      memcpy(&a, &in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=423
Status	New

The size of the buffer used by AddressTestIPv6Le05 in Namespace538243107, at line 985 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6Le05 passes to Namespace538243107, at line 985 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	999	999
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6Le05(void)

```
....
999.      memcpy(&b, &in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=424
Status	New

The size of the buffer used by AddressTestIPv6Ge05 in Namespace538243107, at line 1059 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6Ge05 passes to Namespace538243107, at line 1059 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination

File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1069	1069
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6Ge05(void)

```
....
1069.       memcpy(&a, &in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=425
Status New

The size of the buffer used by AddressTestIPv6Ge05 in Namespace538243107, at line 1059 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6Ge05 passes to Namespace538243107, at line 1059 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1073	1073
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6Ge05(void)

```
....
1073.       memcpy(&b, &in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=426
Status New

The size of the buffer used by AddressTestIPv6SubOne01 in Namespace538243107, at line 1081 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6SubOne01

passes to Namespace538243107, at line 1081 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1090	1090
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6SubOne01(void)

```
....
1090.       memcpy(a, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=427
Status	New

The size of the buffer used by AddressTestIPv6SubOne01 in Namespace538243107, at line 1081 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6SubOne01 passes to Namespace538243107, at line 1081 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1101	1101
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6SubOne01(void)

```
....
1101.       memcpy(a, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=428
Status	New

The size of the buffer used by AddressTestIPv6SubOne02 in Namespace538243107, at line 1110 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6SubOne02 passes to Namespace538243107, at line 1110 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1119	1119
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6SubOne02(void)

```
....
1119.       memcpy(a, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=429
Status New

The size of the buffer used by AddressTestIPv6SubOne02 in Namespace538243107, at line 1110 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6SubOne02 passes to Namespace538243107, at line 1110 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1130	1130
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6SubOne02(void)

```
....
1130.       memcpy(a, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=430
Status	New

The size of the buffer used by AddressTestIPv6AddOne01 in Namespace538243107, at line 1139 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddOne01 passes to Namespace538243107, at line 1139 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1148	1148
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddOne01(void)

```
....
1148.       memcpy(a, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=431
Status	New

The size of the buffer used by AddressTestIPv6AddOne01 in Namespace538243107, at line 1139 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddOne01 passes to Namespace538243107, at line 1139 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1159	1159
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddOne01(void)

```
....
1159.       memcpy(a, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=432
Status	New

The size of the buffer used by AddressTestIPv6AddOne02 in Namespace538243107, at line 1168 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddOne02 passes to Namespace538243107, at line 1168 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1177	1177
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddOne02(void)

```
....
1177.       memcpy(a, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=433
Status	New

The size of the buffer used by AddressTestIPv6AddOne02 in Namespace538243107, at line 1168 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddOne02 passes to Namespace538243107, at line 1168 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1188	1188
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddOne02(void)

```
....
1188.       memcpy(a, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=434
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1209	1209
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1209.      memcpy(&a->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=435
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1212	1212
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1212.      memcpy(&a->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=436
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1215	1215
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1215.      memcpy(&b->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=437
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1218	1218
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1218.      memcpy(&b->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=438
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1223	1223
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1223.      memcpy(&a->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=439
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c

Line	1226	1226
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1226.      memcpy(&a->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=440
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1229	1229
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1229.      memcpy(&b->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=441
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1232	1232
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1232.      memcpy(&b->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=442
Status New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1237	1237
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1237.      memcpy(&a->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=443
Status New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the

buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1240	1240
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1240.      memcpy(&a->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=444
Status New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1243	1243
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1243.      memcpy(&b->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=445
Status New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1246	1246
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1246.      memcpy(&b->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=446
Status New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1251	1251
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1251.      memcpy(&a->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=447
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1254	1254
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1254.      memcpy(&a->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=448
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1257	1257
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1257.      memcpy(&b->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=449
Status	New

The size of the buffer used by AddressTestIPv6AddressCmp01 in Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that AddressTestIPv6AddressCmp01 passes to Namespace538243107, at line 1197 of OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c, to overwrite the target buffer.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1260	1260
Object	Namespace538243107	Namespace538243107

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6AddressCmp01(void)

```
....
1260.      memcpy(&b->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

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=1020047&projectid=20040&pathid=1367
Status	New

The buffer allocated by j in nothings@@stb-newest-CVE-2021-3520-FP.c at line 3248 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	3269	3379

Object	4	j

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static stbi_uc *tga_load(stbi *s, int *x, int *y, int *comp, int req_comp)

```
....
3269.     unsigned char raw_data[4];
....
3379.                     raw_data[j] = get8u(s);
```

Buffer Overflow Loops\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1368
Status New

The buffer allocated by j in nothings@@stb-newest-CVE-2021-3520-FP.c at line 3248 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	3269	3372
Object	4	j

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static stbi_uc *tga_load(stbi *s, int *x, int *y, int *comp, int req_comp)

```
....
3269.     unsigned char raw_data[4];
....
3372.                     raw_data[j] = tga_palette[pal_idx+j];
```

Buffer Overflow Loops\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1369
Status New

The buffer allocated by c in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-	ONLYOFFICE@@core-v5.4.99.1786-CVE-

	2022-29776-FP.c	2022-29776-FP.c
Line	975	1033
Object	0	c

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1370
Status New

The buffer allocated by c in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2499	2507
Object	0	c

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1371
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3109
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1372
Status New

The buffer allocated by ddft in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3055
Object	2	ddft

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1373
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3109
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1374
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3110
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1375

Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3110
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1376
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3155
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 11:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1377
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3155
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1378
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3156
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 13:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1379
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3156
Object	2	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1380
Status	New

The buffer allocated by c in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3170
Object	2	c

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1381
Status	New

The buffer allocated by c in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3170
Object	2	c

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1382
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3109
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1383
Status	New

The buffer allocated by ddft in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3055
Object	3	ddft

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1384
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3109
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1385
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3110
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1386
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3110

Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1387
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3155
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1388
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-	ONLYOFFICE@@core-v5.4.99.1786-CVE-

	2022-29776-FP.c	2022-29776-FP.c
Line	3018	3155
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1389
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3156
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1390
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3156
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1391
Status New

The buffer allocated by c in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3170
Object	3	c

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1392
Status New

The buffer allocated by c in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3170
Object	3	c

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1393
Status New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3109
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20

	040&pathid=1394
Status	New

The buffer allocated by ddft in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3055
Object	3	ddft

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1395
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3109
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 30:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1396
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3110
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1397
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3110
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1398
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3155
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1399
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3155
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1400
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3156
Object	3	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1401
Status	New

The buffer allocated by i in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3156
Object	3	i

Code Snippet

File Name	ONLYOFFICE@@core-v5.4.99.1786-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 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1402
Status	New

The buffer allocated by c in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3170
Object	3	c

Code Snippet

File Name	ONLYOFFICE@@core-v5.4.99.1786-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 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1403
Status	New

The buffer allocated by c in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3018	3170

Object	3	c

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1404
Status	New

The buffer allocated by gmb_cam in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3639
Object	4	gmb_cam

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1405
Status	New

The buffer allocated by gmb_cam in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3636
Object	4	gmb_cam

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1406
Status New

The buffer allocated by sq in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3639
Object	4	sq

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1407
Status New

The buffer allocated by k in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3649
Object	4	k

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1408
Status New

The buffer allocated by gmb_cam in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3639
Object	24	gmb_cam

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20

	040&pathid=1409
Status	New

The buffer allocated by gmb_cam in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3636
Object	24	gmb_cam

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1410
Status	New

The buffer allocated by sq in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3639
Object	24	sq

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 45:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1411
Status	New

The buffer allocated by k in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3649
Object	24	k

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1412
Status	New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3641
Object	3	gmb_xyz

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1413
Status	New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3640
Object	3	gmb_xyz

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1414
Status	New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3642
Object	3	gmb_xyz

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1415
Status	New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3641
Object	24	gmb_xyz

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1416
Status	New

The buffer allocated by gmb_xyz in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3625	3640
Object	24	gmb_xyz

Code Snippet

File Name	ONLYOFFICE@@core-v5.4.99.1786-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];
```

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=1020047&projectid=20040&pathid=3489
Status	New

The variable declared in tga_palette at nothings@@stb-newest-CVE-2021-3520-FP.c in line 3248 is not initialized when it is used by tga_palette at nothings@@stb-newest-CVE-2021-3520-FP.c in line 3248.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	3267	3372
Object	tga_palette	tga_palette

Code Snippet

File Name	nothings@@stb-newest-CVE-2021-3520-FP.c
Method	static stbi_uc *tga_load(stbi *s, int *x, int *y, int *comp, int req_comp)

```
....
3267.     unsigned char *tga_palette = NULL;
....
3372.                     raw_data[j] = tga_palette[pal_idx+j];
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3490
Status	New

The variable declared in decaps_iph at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 3751 is not initialized when it is used by decaps_iph at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 3751.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3754	3816
Object	decaps_iph	decaps_iph

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method static int ndpi_init_packet_header(struct ndpi_detection_module_struct *ndpi_str,

```
....
3754.    const struct ndpi_iphdr *decaps_iph = NULL;
....
3816.      ndpi_detection_get_l4_internal(ndpi_str, (const u_int8_t *)
decaps_iph, l3len, &l4ptr, &l4len, &l4protocol, 0);
```

Use of Zero Initialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3491
Status New

The variable declared in EPOCH at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 6478 is not initialized when it is used by EPOCH at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 6478.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	6482	6493
Object	EPOCH	EPOCH

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method int gettimeofday(struct timeval * tp, struct timezone * tzp) {

```
....
6482.    static const uint64_t EPOCH = ((uint64_t)
116444736000000000ULL);
....
6493.    tp->tv_sec  = (long) ((time - EPOCH) / 10000000L);
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=3492
Status	New

The variable declared in saveptr at OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c in line 202 is not initialized when it is used by tok at OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c in line 202.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	210	216
Object	saveptr	tok

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static DetectAsn1Data *DetectAsn1Parse(const char *instr)

```
....
210.      char *saveptr = NULL;
....
216.      tok = strtok_r(asn1str, ASN_DELIM, &saveptr);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3493
Status	New

The variable declared in b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1675 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1678	1696
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot02(void)

```
....
1678.      DetectAddress *b = NULL;
....
1696.      result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3494
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	733	1696
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot02(void)

```
....
1696.      result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3495
Status	New

The variable declared in b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1725 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1728	1746
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1728.       DetectAddress *b = NULL;
....
1746.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3496
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	733	1746
Object	Pointer	b

Code Snippet

File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c

Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c

Method static int AddressTestIPv6CutNot03(void)

```
....
1746.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3497
Status	New

The variable declared in b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775.

	Source	Destination

File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1778	1804
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1778.       DetectAddress *b = NULL;
....
1804.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3498
Status New

The variable declared in Pointer at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	733	1804
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1804.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 11:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3499
Status	New

The variable declared in b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1836	1862
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1836.       DetectAddress *b = NULL;
....
1862.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3500
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	733	1862
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c

Method	static int AddressTestIPv6CutNot05(void)

```
....
1862.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3501
Status	New

The variable declared in b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1675 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1678	1696
Object	b	b

Code Snippet	
File Name	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method	static int AddressTestIPv6CutNot02(void)

```
....
1678.       DetectAddress *b = NULL;
....
1696.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3502
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	733	1696
Object	Pointer	b

Code Snippet

File Name	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method	int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.        *b = NULL;
```

File Name	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method	static int AddressTestIPv6CutNot02(void)

```
....
1696.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3503
Status	New

The variable declared in b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1725 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1728	1746
Object	b	b

Code Snippet

File Name	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method	static int AddressTestIPv6CutNot03(void)

```
....
1728.       DetectAddress *b = NULL;
....
1746.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3504
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	733	1746
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c

Method static int AddressTestIPv6CutNot03(void)

```
....
1746.      result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3505
Status	New

The variable declared in b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1778	1804
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1778.      DetectAddress *b = NULL;
....
1804.      result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3506
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	733	1804
Object	Pointer	b

Code Snippet

File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c

Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c

Method static int AddressTestIPv6CutNot04(void)

```
....
1804.      result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3507
Status	New

The variable declared in b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1836	1862
Object	b	b

Code Snippet

File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c

Method static int AddressTestIPv6CutNot05(void)

```
....
1836.       DetectAddress *b = NULL;
....
1862.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3508
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	733	1862
Object	Pointer	b

Code Snippet

File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c

Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c

Method static int AddressTestIPv6CutNot05(void)

```
....
1862.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3509
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1675 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1675.

	Source	Destination

File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	1678	1696
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method static int AddressTestIPv6CutNot02(void)

```
....
1678.       DetectAddress *b = NULL;
....
1696.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3510
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	733	1696
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c

Method static int AddressTestIPv6CutNot02(void)

```
....
1696.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3511
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1725 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	1728	1746
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1728.       DetectAddress *b = NULL;
....
1746.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3512
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	733	1746
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method	static int AddressTestIPv6CutNot03(void)

```
....
1746.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3513
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1775 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	1778	1804
Object	b	b

Code Snippet

File Name	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method	static int AddressTestIPv6CutNot04(void)

```
....
1778.       DetectAddress *b = NULL;
....
1804.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3514
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	733	1804
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c

Method static int AddressTestIPv6CutNot04(void)

```
....
1804.      result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3515
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1833 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	1836	1862
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1836.      DetectAddress *b = NULL;
....
1862.      result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3516
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	733	1862
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c

Method static int AddressTestIPv6CutNot05(void)

```
....
1862.      result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3517
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1675 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Line	1678	1696
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot02(void)

```
....
1678.       DetectAddress *b = NULL;
....
1696.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3518
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Line	733	1696
Object	Pointer	b

Code Snippet

File Name OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c

Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c

Method static int AddressTestIPv6CutNot02(void)

```
....
1696.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3519
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1725 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1725.

	Source	Destination

File	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Line	1728	1746
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1728.       DetectAddress *b = NULL;
....
1746.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3520
Status New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Line	733	1746
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1746.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 33:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3521
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Line	1778	1804
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1778.       DetectAddress *b = NULL;
....
1804.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3522
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Line	733	1804
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c

Method	static int AddressTestIPv6CutNot04(void)

```
....
1804.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3523
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Line	1836	1862
Object	b	b

Code Snippet

File Name	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Method	static int AddressTestIPv6CutNot05(void)

```
....
1836.       DetectAddress *b = NULL;
....
1862.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3524
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Line	733	1862
Object	Pointer	b

Code Snippet

File Name	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Method	int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.        *b = NULL;
```

File Name	OISF@@suricata-suricata-6.0.1-CVE-2023-35853-TP.c
Method	static int AddressTestIPv6CutNot05(void)

```
....
1862.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3525
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1675 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Line	1678	1696
Object	b	b

Code Snippet

File Name	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Method	static int AddressTestIPv6CutNot02(void)

```
....
1678.       DetectAddress *b = NULL;
....
1696.       result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3526
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Line	733	1696
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c

Method static int AddressTestIPv6CutNot02(void)

```
....
1696.      result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3527
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1725 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Line	1728	1746
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1728.      DetectAddress *b = NULL;
....
1746.      result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3528
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Line	733	1746
Object	Pointer	b

Code Snippet

File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c

Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c

Method static int AddressTestIPv6CutNot03(void)

```
....
1746.      result &= (b == NULL);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3529
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Line	1778	1804
Object	b	b

Code Snippet

File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c

Method static int AddressTestIPv6CutNot04(void)

```
....
1778.       DetectAddress *b = NULL;
....
1804.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3530
Status	New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Line	733	1804
Object	Pointer	b

Code Snippet

File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c

Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c

Method static int AddressTestIPv6CutNot04(void)

```
....
1804.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3531
Status	New

The variable declared in b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1833.

	Source	Destination

File	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Line	1836	1862
Object	b	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1836.       DetectAddress *b = NULL;
....
1862.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3532
Status New

The variable declared in Pointer at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 723 is not initialized when it is used by b at OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c	OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Line	733	1862
Object	Pointer	b

Code Snippet
File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Method int DetectAddressCutNotIPv6(DetectAddress *a, DetectAddress **b)

```
....
733.       *b = NULL;
```

File Name OISF@@suricata-suricata-6.0.5-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1862.       result &= (b != NULL);
```

Use of Zero Initialized Pointer\Path 45:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3533
Status	New

The variable declared in ssh at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 156 is not initialized when it is used by ssh at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 220.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	158	228
Object	ssh	ssh

Code Snippet

File Name OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c

Method static DetectSshSoftwareVersionData *DetectSshSoftwareVersionParse (DetectEngineCtx *de_ctx, const char *str)

```
....
158.      DetectSshSoftwareVersionData *ssh = NULL;
```

File Name OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c

Method static int DetectSshSoftwareVersionSetup (DetectEngineCtx *de_ctx, Signature *s, const char *str)

```
....
228.      ssh = DetectSshSoftwareVersionParse(NULL, str);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3534
Status	New

The variable declared in ssh at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 156 is not initialized when it is used by ssh at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 276.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	158	279
Object	ssh	ssh

Code Snippet

File Name OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c

Method	static DetectSshSoftwareVersionData *DetectSshSoftwareVersionParse (DetectEngineCtx *de_ctx, const char *str)

```
....
158.      DetectSshSoftwareVersionData *ssh = NULL;
```

File Name	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Method	static int DetectSshSoftwareVersionTestParse01 (void)

```
....
279.      ssh = DetectSshSoftwareVersionParse(NULL, "PuTTY_1.0");
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3535
Status	New

The variable declared in ssh at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 156 is not initialized when it is used by ssh at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 292.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	158	295
Object	ssh	ssh

Code Snippet

File Name	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Method	static DetectSshSoftwareVersionData *DetectSshSoftwareVersionParse (DetectEngineCtx *de_ctx, const char *str)

```
....
158.      DetectSshSoftwareVersionData *ssh = NULL;
```

File Name	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Method	static int DetectSshSoftwareVersionTestParse02 (void)

```
....
295.      ssh = DetectSshSoftwareVersionParse(NULL, "\"SecureCRT-
4.0\"");
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3536
Status	New

The variable declared in ssh at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 156 is not initialized when it is used by ssh at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 308.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	158	311
Object	ssh	ssh

Code Snippet

File Name OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c

Method static DetectSshSoftwareVersionData *DetectSshSoftwareVersionParse (DetectEngineCtx *de_ctx, const char *str)

```
....
158.      DetectSshSoftwareVersionData *ssh = NULL;
```

File Name OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c

Method static int DetectSshSoftwareVersionTestParse03 (void)

```
....
311.      ssh = DetectSshSoftwareVersionParse(NULL, "");
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3537
Status	New

The variable declared in ssh at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 156 is not initialized when it is used by ssh at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 156.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	158	179
Object	ssh	ssh

Code Snippet

File Name OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c

Method	static DetectSshSoftwareVersionData *DetectSshSoftwareVersionParse (DetectEngineCtx *de_ctx, const char *str)

```
....
158.      DetectSshSoftwareVersionData *ssh = NULL;
....
179.          ssh = SCMalloc(sizeof(DetectSshSoftwareVersionData));
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3538
Status	New

The variable declared in str_ptr at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 156 is not initialized when it is used by str_ptr at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 156.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	171	189
Object	str_ptr	str_ptr

Code Snippet	
File Name	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Method	static DetectSshSoftwareVersionData *DetectSshSoftwareVersionParse (DetectEngineCtx *de_ctx, const char *str)

```
....
171.          const char *str_ptr = NULL;
....
189.          pcre2_substring_free((PCRE2_UCHAR *)str_ptr);
```

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=1020047&projectid=20040&pathid=3565
Status	New

The size of the buffer used by kodak_radc_load_raw in buf, at line 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	buf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3566
Status	New

The size of the buffer used by kodak_radc_load_raw in sizeof, at line 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3567
Status	New

The size of the buffer used by kodak_radc_load_raw in BinaryExpr, at line 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	BinaryExpr

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3568

Status	New

The size of the buffer used by kodak_radc_load_raw in sizeof, at line 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3569
Status	New

The size of the buffer used by kodak_radc_load_raw in c, at line 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	c

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3570
Status	New

The size of the buffer used by kodak_radc_load_raw in c, at line 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	c

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3571

Status	New

The size of the buffer used by kodak_radc_load_raw in BinaryExpr, at line 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	BinaryExpr

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3572
Status	New

The size of the buffer used by kodak_radc_load_raw in buf, at line 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	buf

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3573
Status	New

The size of the buffer used by ljpeg_start in Pointer, at line 823 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	Pointer

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3574

Status	New

The size of the buffer used by ljpeg_start in jh, at line 823 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	jh

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3575
Status	New

The size of the buffer used by ljpeg_start in sizeof, at line 823 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3576
Status	New

The size of the buffer used by canon_compressed_load_raw in diffbuf, at line 737 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	758
Object	fgetc	diffbuf

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method void CLASS canon_compressed_load_raw()

```
....
758.        memset (diffbuf, 0, sizeof diffbuf);
```

Stored Buffer Overflow boundcpy\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3577

Status	New

The size of the buffer used by canon_compressed_load_raw in sizeof, at line 737 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	758
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method void CLASS canon_compressed_load_raw()

```
....
758.        memset (diffbuf, 0, sizeof diffbuf);
```

Stored Buffer Overflow boundcpy\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3578
Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2416	2505
Object	fgetc	rgb

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2416.       c = fgetc(ifp);
```

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3579
Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2432	2505
Object	fgetc	rgb

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2432.       bitbuf += fgetc(ifp);
```

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3580

Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	344	2505
Object	pixel	rgb

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-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=1020047&projectid=20040&pathid=3581
Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2416	2505
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2416.       c = fgetc(ifp);
```

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3582
Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2432	2505
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2432.       bitbuf += fgetc(ifp);
```

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3583

Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	344	2505
Object	pixel	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-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=1020047&projectid=20040&pathid=3584
Status	New

The size of the buffer used by canon_compressed_load_raw in diffbuf, at line 737 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	758
Object	fgetc	diffbuf

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method void CLASS canon_compressed_load_raw()

```
....
758.        memset (diffbuf, 0, sizeof diffbuf);
```

Stored Buffer Overflow boundcpy\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3585
Status	New

The size of the buffer used by canon_compressed_load_raw in sizeof, at line 737 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	758
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method void CLASS canon_compressed_load_raw()

```
....
758.        memset (diffbuf, 0, sizeof diffbuf);
```

Stored Buffer Overflow boundcpy\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3586

Status	New

The size of the buffer used by ljpeg_start in Pointer, at line 823 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	Pointer

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3587
Status	New

The size of the buffer used by ljpeg_start in jh, at line 823 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	jh

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3588
Status	New

The size of the buffer used by ljpeg_start in sizeof, at line 823 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	829
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3589

Status	New

The size of the buffer used by kodak_radc_load_raw in buf, at line 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	buf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3590
Status	New

The size of the buffer used by kodak_radc_load_raw in sizeof, at line 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3591
Status	New

The size of the buffer used by kodak_radc_load_raw in BinaryExpr, at line 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	BinaryExpr

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3592

Status	New

The size of the buffer used by kodak_radc_load_raw in sizeof, at line 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3593
Status	New

The size of the buffer used by kodak_radc_load_raw in c, at line 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	c

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3594
Status	New

The size of the buffer used by kodak_radc_load_raw in c, at line 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	c

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3595

Status	New

The size of the buffer used by kodak_radc_load_raw in BinaryExpr, at line 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3596
Status	New

The size of the buffer used by kodak_radc_load_raw in buf, at line 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	585	2214
Object	fgetc	buf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

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

File Name ONLYOFFICE@@core-v5.5.2.2-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 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3597
Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2416	2505
Object	fgetc	rgb

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2416.      c = fgetc(ifp);
```

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3598

Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2432	2505
Object	fgetc	rgb

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2432.       bitbuf += fgetc(ifp);
```

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.         memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3599
Status	New

The size of the buffer used by kodak_rgb_load_raw in rgb, at line 2495 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	344	2505
Object	pixel	rgb

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3600
Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2416	2505
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2416.      c = fgetc(ifp);
```

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3601

Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2432	2505
Object	fgetc	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2432.       bitbuf += fgetc(ifp);
```

File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.         memset (rgb, 0, sizeof rgb);
```

Stored Buffer Overflow boundcpy\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3602
Status	New

The size of the buffer used by kodak_rgb_load_raw in sizeof, at line 2495 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	344	2505
Object	pixel	sizeof

Code Snippet

File Name ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c

Method void CLASS kodak_rgb_load_raw()

```
....
2505.        memset (rgb, 0, sizeof rgb);
```

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=1020047&projectid=20040&pathid=1487
Status	New

The application performs an illegal operation in canon_a5_load_raw, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 548.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	566	566
Object	bc	bc

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1488
Status	New

The application performs an illegal operation in canon_a5_load_raw, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 548.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	566	566
Object	bc	bc

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1489
Status New

The application performs an illegal operation in process_frame_header, in nothings@@stb-newest-CVE-2021-3520-FP.c. In line 1544, the program attempts to divide by img_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 img_n in process_frame_header of nothings@@stb-newest-CVE-2021-3520-FP.c, at line 1544.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	1575	1575
Object	img_n	img_n

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static int process_frame_header(jpeg *z, int scan)

```
....
1575.     if ((1 << 30) / s->img_x / s->img_n < s->img_y) return e("too
large", "Image too large to decode");
```

Divide By Zero\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1490
Status	New

The application performs an illegal operation in main, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8559	8559
Object	pixel_aspect	pixel_aspect

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1491
Status	New

The application performs an illegal operation in remove_zeroes, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 520.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	533	533
Object	n	n

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS remove_zeroes()

```
....
533.        if (n) BAYER(row,col) = tot/n;
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1492
Status	New

The application performs an illegal operation in main, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8559	8559
Object	pixel_aspect	pixel_aspect

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1493
Status	New

The application performs an illegal operation in remove_zeroes, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 520.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	533	533
Object	n	n

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS remove_zeroes()

```
....
533.        if (n) BAYER(row,col) = tot/n;
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1494
Status	New

The application performs an illegal operation in foveon_interpolate, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 3014.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3079	3079
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3079.    FORC3 div[c] /= num;
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1495
Status	New

The application performs an illegal operation in cam_xyz_coeff, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 3545.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3559	3559
Object	num	num

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-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 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1496
Status	New

The application performs an illegal operation in scale_colors, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 3748.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3812	3812
Object	dmax	dmax

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-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 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1497
Status	New

The application performs an illegal operation in foveon_interpolate, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 3014.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Line	3079	3079
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3079.    FORC3 div[c] /= num;
```

Divide By Zero\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1498
Status	New

The application performs an illegal operation in cam_xyz_coeff, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 3545.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3559	3559
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1499
Status	New

The application performs an illegal operation in scale_colors, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 3748.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3812	3812
Object	dmax	dmax

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1500
Status New

The application performs an illegal operation in foveon_make_curve, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 2976.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2983	2983
Object	filt	filt

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1501
Status New

The application performs an illegal operation in foveon_make_curve, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 2976.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2989	2989
Object	max	max

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1502
Status New

The application performs an illegal operation in bad_pixels, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 3417.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3465	3465
Object	n	n

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3465.       BAYER2(row,col) = tot/n;
```

Divide By Zero\Path 17:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1503
Status	New

The application performs an illegal operation in cam_xyz_coeff, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 3545.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3560	3560
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1504
Status	New

The application performs an illegal operation in scale_colors, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 3748.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3812	3812
Object	maximum	maximum

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1505
Status	New

The application performs an illegal operation in vng_interpolate, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 3962.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4073	4073
Object	num	num

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method	void CLASS vng_interpolate()

```
....
4073.          t += (sum[c] - sum[color]) / num;
```

Divide By Zero\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1506
Status	New

The application performs an illegal operation in recover_highlights, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 4339.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4373	4373
Object	wgt	wgt

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method	void CLASS recover_highlights()

```
....
4373.          map[mrow*wide+mcol] = sum / wgt;
```

Divide By Zero\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1507
Status	New

The application performs an illegal operation in gamma_lut, in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, at line 8111.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8126	8126
Object	white	white

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS gamma_lut (uchar lut[0x10000])

```
....
8126.       r = i / white;
```

Divide By Zero\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1508
Status	New

The application performs an illegal operation in foveon_make_curve, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 2976.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2983	2983
Object	filt	filt

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.2.2-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 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1509
Status	New

The application performs an illegal operation in foveon_make_curve, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 2976.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2989	2989
Object	max	max

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.2.2-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 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1510
Status	New

The application performs an illegal operation in bad_pixels, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 3417.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Line	3465	3465
Object	n	n

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3465.       BAYER2(row,col) = tot/n;
```

Divide By Zero\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1511
Status	New

The application performs an illegal operation in cam_xyz_coeff, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 3545.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3560	3560
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1512
Status	New

The application performs an illegal operation in scale_colors, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 3748.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3812	3812
Object	maximum	maximum

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1513
Status New

The application performs an illegal operation in vng_interpolate, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 3962.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4073	4073
Object	num	num

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS vng_interpolate()

```
....
4073.            t += (sum[c] - sum[color]) / num;
```

Divide By Zero\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1514
Status New

The application performs an illegal operation in recover_highlights, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 4339.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4373	4373
Object	wgt	wgt

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS recover_highlights()

```
....
4373.          map[mrow*wide+mcol] = sum / wgt;
```

Divide By Zero\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1515
Status	New

The application performs an illegal operation in gamma_lut, in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, at line 8111.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8126	8126
Object	white	white

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS gamma_lut (uchar lut[0x10000])

```
....
8126.       r = i / white;
```

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=1020047&projectid=20040&pathid=3255
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	18	49
Object	scratch_buffer	scratch_buffer

Code Snippet

File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c

Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
49.              message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3256
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	18	56
Object	scratch_buffer	scratch_buffer

Code Snippet

File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c

Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
56.              message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3257
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	18	52
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
52.                      scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3258
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	18	54
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
54.                      scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3259
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	18	46
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
46.          if ((uint8_t*)request >= scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3260
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	18	47
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
47.              && (uint8_t*)request < scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3261
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	21	42
Object	sender_buffer	sender_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
42.          message = sender_buffer;
```

Use of Uninitialized Variable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3262
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	21	40
Object	sender_buffer	sender_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
40.      if ((uint8_t*) request >= sender_buffer &&
```

Use of Uninitialized Variable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3263
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	21	41
Object	sender_buffer	sender_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
41.          (uint8_t*)request < sender_buffer + sender_buffer_size) {
```

Use of Uninitialized Variable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3264
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	122	159
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_receive_response(void *context, const uint32_t *session_id,

```
....
122.      uint8_t *scratch_buffer;
....
159.      *response = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SECURE_MESSAGE_OFFSET +
```

Use of Uninitialized Variable\Path 11:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3265
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	296	326
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
296.      uint8_t *scratch_buffer;
....
326.      send_info->large_message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_MESSAGE_OFFSET;
```

Use of Uninitialized Variable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3266
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Line	296	318
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.104.12-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
296.      uint8_t *scratch_buffer;
....
318.      message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3267
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	18	49
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
49.              message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3268
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	18	56
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
56.              message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 15:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3269
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	18	52
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
52.                      scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3270
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	18	54
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
54.                      scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 17:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3271
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	18	46
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
46.          if ((uint8_t*)request >= scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3272
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	18	47
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
18.      uint8_t *scratch_buffer;
....
47.              && (uint8_t*)request < scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 19:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3273
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	21	42
Object	sender_buffer	sender_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
42.          message = sender_buffer;
```

Use of Uninitialized Variable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3274
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	21	40
Object	sender_buffer	sender_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
40.      if ((uint8_t*) request >= sender_buffer &&
```

Use of Uninitialized Variable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3275

Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	21	41
Object	sender_buffer	sender_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
21.      uint8_t *sender_buffer;
....
41.          (uint8_t*)request < sender_buffer + sender_buffer_size) {
```

Use of Uninitialized Variable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3276
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	122	159
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_receive_response(void *context, const uint32_t *session_id,

```
....
122.      uint8_t *scratch_buffer;
....
159.      *response = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SECURE_MESSAGE_OFFSET +
```

Use of Uninitialized Variable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3277
Status	New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	296	326
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
296.      uint8_t *scratch_buffer;
....
326.      send_info->large_message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_MESSAGE_OFFSET;
```

Use of Uninitialized Variable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3278
Status New

	Source	Destination
File	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c	NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Line	296	318
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name NVIDIA@@open-gpu-kernel-modules-535.43.23-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
296.      uint8_t *scratch_buffer;
....
318.      message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3279
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3676	3717
Object	lpass	lpass

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3280
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3676	3717
Object	lpass	lpass

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3281
Status New

	Source	Destination

File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3676	3717
Object	lpass	lpass

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3282
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3676	3717
Object	lpass	lpass

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 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=1020047&projectid=20040&pathid=3231
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	628	642
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3232
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	628	633
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3233
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	628	644
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3234
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by leaf at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	628	647
Object	cur	leaf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3235
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2105	2109
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3236
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2105	2107
Object	cur	cur

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3237
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2105	2111
Object	cur	branch

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3238
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by leaf at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-	ONLYOFFICE@@core-v5.4.99.1786-CVE-

	2022-29776-FP.c	2022-29776-FP.c
Line	2105	2114
Object	cur	leaf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3239
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by leaf at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2775	2791
Object	cur	leaf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3240
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2775	2783
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3241
Status New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2775	2797
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3242
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2775	2799
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3243
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	628	642
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3244
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	628	633
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3245
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	628	644
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3246
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 626 is not initialized when it is used by leaf at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 626.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	628	647
Object	cur	leaf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3247
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2105	2109
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3248
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2105	2107
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3249
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2105	2111
Object	cur	branch

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3250
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2103 is not initialized when it is used by leaf at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2103.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2105	2114
Object	cur	leaf

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3251
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by leaf at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2775	2791
Object	cur	leaf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3252
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2775	2783
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3253
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by branch at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c

Line	2775	2797
Object	cur	branch

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3254
Status	New

The variable declared in cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2772 is not initialized when it is used by cur at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 2772.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2775	2799
Object	cur	cur

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS foveon_decoder (unsigned size, unsigned code)

```
....
2775.    struct decode *cur;
....
2799.    cur->branch[1] = free_decode;
```

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=1020047&projectid=20040&pathid=1531
Status	New

The function len in OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c
Line	220	220
Object	len	len

Code Snippet
File Name OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
220.          connp->out_buf = malloc(len);
```

Wrong Size t Allocation\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1532
Status New

The function len in OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c
Line	220	220
Object	len	len

Code Snippet
File Name OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
220.          connp->out_buf = malloc(len);
```

Wrong Size t Allocation\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1533
Status New

The function len in OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c
Line	220	220
Object	len	len

Code Snippet
File Name OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
220.          connp->out_buf = malloc(len);
```

Wrong Size t Allocation\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1534
Status New

The function len in OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c
Line	220	220
Object	len	len

Code Snippet
File Name OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
220.          connp->out_buf = malloc(len);
```

Wrong Size t Allocation\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1535

Status	New

The function len in OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c
Line	220	220
Object	len	len

Code Snippet
File Name OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
220.          connp->out_buf = malloc(len);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1536
Status	New

The function len in OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c
Line	220	220
Object	len	len

Code Snippet
File Name OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
220.          connp->out_buf = malloc(len);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=1537
Status	New

The function len in OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c at line 191 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	OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c
Line	219	219
Object	len	len

Code Snippet
File Name OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_req_buffer(htp_connp_t *connp) {

```
....
219.          connp->in_buf = malloc(len);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1538
Status	New

The function len in OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c at line 191 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	OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c
Line	219	219
Object	len	len

Code Snippet
File Name OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_req_buffer(htp_connp_t *connp) {

```
....
219.          connp->in_buf = malloc(len);
```

Wrong Size t Allocation\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1539
Status	New

The function newsize in OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c
Line	226	226
Object	newsize	newsize

Code Snippet
File Name OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
226.          unsigned char *newbuf = realloc(connp->out_buf, newsize);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1540
Status	New

The function newsize in OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c
Line	226	226
Object	newsize	newsize

Code Snippet
File Name OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
226.          unsigned char *newbuf = realloc(connp->out_buf, newsize);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1541
Status	New

The function newsize in OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c
Line	226	226
Object	newsize	newsize

Code Snippet
File Name OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
226.          unsigned char *newbuf = realloc(connp->out_buf, newsize);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1542
Status	New

The function newsize in OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c
Line	226	226
Object	newsize	newsize

Code Snippet
File Name OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
226.          unsigned char *newbuf = realloc(connp->out_buf, newsize);
```

Wrong Size t Allocation\Path 13:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1543
Status	New

The function newsize in OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c
Line	226	226
Object	newsize	newsize

Code Snippet
File Name OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
226.          unsigned char *newbuf = realloc(connp->out_buf, newsize);
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1544
Status	New

The function newsize in OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c at line 195 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	OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c
Line	226	226
Object	newsize	newsize

Code Snippet
File Name OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_res_buffer(htp_connp_t *connp) {

```
....
226.          unsigned char *newbuf = realloc(connp->out_buf, newsize);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1545
Status	New

The function newsize in OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c at line 191 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	OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c
Line	225	225
Object	newsize	newsize

Code Snippet
File Name OISF@@libhtp-0.5.41-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_req_buffer(htp_connp_t *connp) {

```
....
225.          unsigned char *newbuf = realloc(connp->in_buf, newsize);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1546
Status	New

The function newsize in OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c at line 191 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	OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c
Line	225	225
Object	newsize	newsize

Code Snippet
File Name OISF@@libhtp-0.5.43-CVE-2024-23837-TP.c
Method static htp_status_t htp_connp_req_buffer(htp_connp_t *connp) {

```
....
225.          unsigned char *newbuf = realloc(connp->in_buf, newsize);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1547
Status	New

The function dsize in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2937	2937
Object	dsize	dsize

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1548
Status	New

The function dsize in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2937	2937
Object	dsize	dsize

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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

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=1020047&projectid=20040&pathid=3214
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	2202	2202
Object	ndpi_str	ndpi_str

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method struct ndpi_detection_module_struct *ndpi_init_detection_module(ndpi_init_prefs prefs) {

```
....
2202.    struct ndpi_detection_module_struct *ndpi_str =
ndpi_malloc(sizeof(struct ndpi_detection_module_struct));
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3215
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	88	88
Object	ndpi_malloc	ndpi_malloc

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method void* ndpi_flow_malloc(size_t size) { return(_ndpi_flow_malloc ? _ndpi_flow_malloc(size) : ndpi_malloc(size)); }

```
....
88.  void* ndpi_flow_malloc(size_t size) { return(_ndpi_flow_malloc ?
_ndpi_flow_malloc(size) : ndpi_malloc(size)); }
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3216
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	608	608
Object	ndpi_malloc	ndpi_malloc

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method static int init_hyperscan(struct ndpi_detection_module_struct *ndpi_str) {

```
....
608.    ndpi_str->hyperscan = (void*)ndpi_malloc(sizeof(struct hs));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3217
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	4433	4433
Object	ndpi_malloc	ndpi_malloc

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method int ndpi_load_hostname_category(struct ndpi_detection_module_struct *ndpi_str,

```
....
4433.        struct hs_list *h = (struct
hs_list*)ndpi_malloc(sizeof(struct hs_list));
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3218
Status	New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	905	905
Object	output	output

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static float *ldr_to_hdr(stbi_uc *data, int x, int y, int comp)

```
....
905.     float *output = (float *) malloc(x * y * comp * sizeof(float));
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3219
Status	New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	923	923
Object	output	output

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static stbi_uc *hdr_to_ldr(float *data, int x, int y, int comp)

```
....
923.     stbi_uc *output = (stbi_uc *) malloc(x * y * comp);
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3220
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-11939-TP.c	ntop@@nDPI-3.2-CVE-2020-11939-TP.c
Line	297	297
Object	hassh_buf	hassh_buf

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-11939-TP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
297.        char *hassh_buf = calloc(packet->payload_packet_len,
sizeof(char));
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3221
Status New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-11940-TP.c	ntop@@nDPI-3.2-CVE-2020-11940-TP.c
Line	297	297
Object	hassh_buf	hassh_buf

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-11940-TP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
297.        char *hassh_buf = calloc(packet->payload_packet_len,
sizeof(char));
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3222
Status New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c

Line	1600	1600
Object	raw_data	raw_data

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static int process_frame_header(jpeg *z, int scan)

```
....
1600.         z->img_comp[i].raw_data = malloc(z->img_comp[i].w2 * z-
>img_comp[i].h2+15);
```

Memory Leak\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3223
Status New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	1863	1863
Object	linebuf	linebuf

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static stbi__uint8 *load_jpeg_image(jpeg *z, int *out_x, int *out_y, int *comp, int req_comp)

```
....
1863.            z->img_comp[k].linebuf = (stbi__uint8 *) malloc(z->s-
>img_x + 3);
```

Memory Leak\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3224
Status New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	1881	1881
Object	output	output

Code Snippet	
File Name	nothings@@stb-newest-CVE-2021-3520-FP.c
Method	static stbi__uint8 *load_jpeg_image(jpeg *z, int *out_x, int *out_y, int *comp, int req_comp)

```
....
1881.         output = (stbi__uint8 *) malloc(n * z->s->img_x * z->s-
>img_y + 1);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3225
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	870	870
Object	row	row

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-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 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3226
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2985	2985
Object	curve	curve

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-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 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3227
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	870	870
Object	row	row

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3228
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2985	2985
Object	curve	curve

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 16:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3229
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2937	2937
Object	size	size

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3230
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2937	2937
Object	size	size

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void * CLASS foveon_camf_matrix (unsigned dim[3], const char *name)

```
....
2937.      mat = (unsigned *) malloc ((size = dsize) * 4);
```

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=1020047&projectid=20040&pathid=1561
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8066 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8079	8079
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1562
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8066 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8091	8091
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1563
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8066 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8079	8079
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1564
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8066 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8091	8091
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1565
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 413 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	419	419
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1566
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1479 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1595	1595
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1567
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1479 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1586	1586
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1568
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4339 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4375	4375
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1569
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8111 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8127	8127
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1570
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 413 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	419	419
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1571
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1479 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	1595	1595
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1572
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1479 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	1586	1586
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20

	040&pathid=1573
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4339 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4375	4375
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1574
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8111 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8127	8127
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS gamma_lut (uchar lut[0x10000])

```
....
8127.       val = 256 * ( !use_gamma ? r :
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1575

Status	New

A variable of a larger data type, idx, is being assigned to a smaller data type, in 41 of ntop@@nDPI-3.4-CVE-2021-36082-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	ntop@@nDPI-3.4-CVE-2021-36082-TP.c	ntop@@nDPI-3.4-CVE-2021-36082-TP.c
Line	42	42
Object	idx	idx

Code Snippet
File Name ntop@@nDPI-3.4-CVE-2021-36082-TP.c
Method int ndpi_netbios_name_interpret(char *in, size_t inlen, char *out, u_int out_len)
{

```
....
42.    int ret = 0, len, idx = inlen;
```

MemoryFree on StackVariable

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

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1516
Status	New

Calling free() (line 529) on a variable that was not dynamically allocated (line 529) in file OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c may result with a crash.

	Source	Destination
File	OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c
Line	598	598
Object	h	h

Code Snippet
File Name OISF@@libhtp-0.5.33-CVE-2024-23837-TP.c
Method htp_status_t htp_connp_RES_BODY_DETERMINE(htp_connp_t *connp) {

```
....
598.                free(h);
```

MemoryFree on StackVariable\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1517
Status	New

Calling free() (line 529) on a variable that was not dynamically allocated (line 529) in file OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c may result with a crash.

	Source	Destination
File	OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c
Line	598	598
Object	h	h

Code Snippet
File Name OISF@@libhtp-0.5.34-CVE-2024-23837-TP.c
Method htp_status_t htp_connp_RES_BODY_DETERMINE(htp_connp_t *connp) {

```
....
598.                free(h);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1518
Status	New

Calling free() (line 544) on a variable that was not dynamically allocated (line 544) in file OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c may result with a crash.

	Source	Destination
File	OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c
Line	616	616
Object	h	h

Code Snippet
File Name OISF@@libhtp-0.5.37-CVE-2024-23837-TP.c
Method htp_status_t htp_connp_RES_BODY_DETERMINE(htp_connp_t *connp) {

```
....
616.                free(h);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=1519
Status	New

Calling free() (line 546) on a variable that was not dynamically allocated (line 546) in file OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c may result with a crash.

	Source	Destination
File	OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c
Line	618	618
Object	h	h

Code Snippet
File Name OISF@@libhtp-0.5.38-CVE-2024-23837-TP.c
Method htp_status_t htp_connp_RES_BODY_DETERMINE(htp_connp_t *connp) {

```
....
618.                free(h);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1520
Status	New

Calling free() (line 546) on a variable that was not dynamically allocated (line 546) in file OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c may result with a crash.

	Source	Destination
File	OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c
Line	618	618
Object	h	h

Code Snippet
File Name OISF@@libhtp-0.5.39-CVE-2024-23837-TP.c
Method htp_status_t htp_connp_RES_BODY_DETERMINE(htp_connp_t *connp) {

```
....
618.                free(h);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1521

Status	New

Calling free() (line 546) on a variable that was not dynamically allocated (line 546) in file OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c may result with a crash.

	Source	Destination
File	OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c	OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c
Line	625	625
Object	h	h

Code Snippet
File Name OISF@@libhtp-0.5.40-CVE-2024-23837-TP.c
Method htp_status_t htp_connp_RES_BODY_DETERMINE(htp_connp_t *connp) {

```
....
625.                    free(h);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1522
Status	New

Calling free() (line 3014) on a variable that was not dynamically allocated (line 3014) in file ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3394	3394
Object	shrink	shrink

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3394.    free (shrink);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1523
Status	New

Calling free() (line 4913) on a variable that was not dynamically allocated (line 4913) in file ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5189	5189
Object	cbuf	cbuf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5189.       free (cbuf);
```

MemoryFree on StackVariable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1524
Status New

Calling free() (line 4913) on a variable that was not dynamically allocated (line 4913) in file ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5302	5302
Object	buf	buf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5302.       free (buf);
```

MemoryFree on StackVariable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1525
Status New

Calling free() (line 3014) on a variable that was not dynamically allocated (line 3014) in file ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3394	3394
Object	shrink	shrink

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS foveon_interpolate()

```
....
3394.    free (shrink);
```

MemoryFree on StackVariable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1526
Status New

Calling free() (line 4913) on a variable that was not dynamically allocated (line 4913) in file ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5189	5189
Object	cbuf	cbuf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5189.        free (cbuf);
```

MemoryFree on StackVariable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1527
Status New

Calling free() (line 4913) on a variable that was not dynamically allocated (line 4913) in file ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c may result with a crash.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5302	5302
Object	buf	buf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5302.       free (buf);
```

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=1020047&projectid=20040&pathid=1549
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3014 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3088	3088
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1550
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3545 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3560	3560
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1551
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3748 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3812	3812
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1552
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4913 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5111	5111
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1553
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8028 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8048	8048
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1554
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8028 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8049	8049
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1555
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3014 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3088	3088
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1556
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3545 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3560	3560
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1557
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3748 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3812	3812
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1558
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4913 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5111	5111
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1559
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8028 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8048	8048
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1560
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 8028 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8049	8049
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1576
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4913 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5203	5203
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1577
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2183	2183
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1578
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2193	2193
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1579
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2199	2199
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1580
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2202	2202
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1581
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4913 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5203	5203
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1582
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2183	2183
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1583
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2193	2193
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1584
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2199	2199
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=1585
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2166 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2202	2202
Object	AssignExpr	AssignExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS kodak_radc_load_raw()

```
....
2202.              FORYX buf[c][y][x] += step;
```

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=1020047&projectid=20040&pathid=3603
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination

File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3604
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3605
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3606
Status New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4831	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3607
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4851	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3608
Status	New

The size of the buffer used by parse_mos in i, at line 4805 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4855	4833
Object	Address	i

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

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

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=1020047&projectid=20040&pathid=388
Status	New

The pointer sum at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 6521 is being used after it has been freed.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	6537	6537
Object	sum	sum

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=389
Status	New

The pointer sum at ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c in line 6521 is being used after it has been freed.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	6537	6537
Object	sum	sum

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=390
Status New

The pointer sum at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 6521 is being used after it has been freed.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	6537	6537
Object	sum	sum

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=391
Status New

The pointer sum at ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c in line 6521 is being used after it has been freed.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	6537	6537
Object	sum	sum

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method short CLASS guess_byte_order (int words)

```
....
6537.    return sum[0] < sum[1] ? 0x4d4d : 0x4949;
```

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=1020047&projectid=20040&pathid=3210
Status	New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	4334	4339
Object	scanline	scanline

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static float *hdr_load(stbi *s, int *x, int *y, int *comp, int req_comp)

```
....
4334.               free(scanline);
....
4339.           if (len != width) { free(hdr_data); free(scanline);
return epf("invalid decoded scanline length", "corrupt HDR"); }
```

Double Free\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3211
Status	New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	4334	4362
Object	scanline	scanline

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static float *hdr_load(stbi *s, int *x, int *y, int *comp, int req_comp)

```
....
4334.               free(scanline);
....
4362.         free(scanline);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3212
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3448	3448
Object	fname	fname

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3448.       free (fname);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3213
Status	New

	Source	Destination

File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3448	3448
Object	fname	fname

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3448.       free (fname);
```

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=1020047&projectid=20040&pathid=1528
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	983	983
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=1529
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	983	983
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS canon_sraw_load_raw()

```
....
983.    for (ecol=slice=0; slice <= cr2_slice[0]; slice++) {
```

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=1020047&projectid=20040&pathid=3283
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Line	147	147
Object	Decode	Decode

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3284
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Line	153	153
Object	Encode	Encode

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(byte *output, size_t outputLen) const

```
....
153.        Encode(sink, outputLen);
```

Off by One Error in Methods

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Methods Version:0

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 Methods\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=1530
Status	New

The buffer allocated by sizeof in ntop@@nDPI-3.2-CVE-2020-15475-TP.c at line 4383 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	4391	4391
Object	ipbuf	sizeof

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method int ndpi_load_ip_category(struct ndpi_detection_module_struct *ndpi_str,

```
....
4391.    strncpy(ipbuf, ip_address_and_mask, sizeof(ipbuf));
```

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=1020047&projectid=20040&pathid=3609
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	1974	1974
Object	fgets	fgets

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method int ndpi_load_ipv4_ptree(struct ndpi_detection_module_struct *ndpi_str,

```
....
1974.      line = fgets(buffer, sizeof(buffer), fd);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3610
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	2863	2863
Object	fgets	fgets

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c

Method	int ndpi_load_categories_file(struct ndpi_detection_module_struct *ndpi_str, const char* path) {

```
....
2863.      line = fgets(buffer, sizeof(buffer), fd);
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3611
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	2935	2935
Object	fgets	fgets

Code Snippet

File Name	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method	int ndpi_load_protocols_file(struct ndpi_detection_module_struct *ndpi_str, const char* path) {

```
....
2935.      while((line = fgets(line, line_len, fd)) != NULL &&
line[strlen(line)-1] != '\n') {
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3612
Status	New

	Source	Destination
File	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Line	271	271
Object	fgets	fgets

Code Snippet

File Name	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Method	static DetectFileHashData *DetectFileHashParse (const DetectEngineCtx *de_ctx,

```
....
271.      while(fgets(line, (int)sizeof(line), fp) != NULL) {
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3613
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3451	3451
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3451.    while (fgets (line, 128, fp)) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3614
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4546	4546
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_makernote (int base, int uptag)

```
....
4546.        fgets (model2, 64, ifp);
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3615

Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4785	4785
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3616
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4977	4977
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4977.       fgets (make, 64, ifp);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3617
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Line	4980	4980
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4980.       fgets (model, 64, ifp);
```

Improper Resource Access Authorization\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3618
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5011	5011
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5011.       fgets (software, 64, ifp);
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3619
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5076	5076
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method	int CLASS parse_tiff_ifd (int base)

```
....
5076.       fgets (model2, 64, ifp);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3620
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5667	5667
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_rollei()

```
....
5667.      fgets (line, 128, ifp);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3621
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3451	3451
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3451.    while (fgets (line, 128, fp)) {
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3622
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4546	4546
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_makernote (int base, int uptag)

```
....
4546.         fgets (model2, 64, ifp);
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3623
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4785	4785
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3624
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4977	4977
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4977.       fgets (make, 64, ifp);
```

Improper Resource Access Authorization\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3625
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4980	4980
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
4980.       fgets (model, 64, ifp);
```

Improper Resource Access Authorization\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3626
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5011	5011

Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5011.       fgets (software, 64, ifp);
```

Improper Resource Access Authorization\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3627
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5076	5076
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5076.       fgets (model2, 64, ifp);
```

Improper Resource Access Authorization\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3628
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5667	5667
Object	fgets	fgets

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_rollei()

```
....
5667.       fgets (line, 128, ifp);
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3629
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4831	4831
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.         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=1020047&projectid=20040&pathid=3630
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4842	4842
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 23:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3631
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4846	4846
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

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

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3632
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4848	4848
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

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

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3633
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4851	4851
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.       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=1020047&projectid=20040&pathid=3634
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4855	4855
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.       fscanf (ifp, "%d", &i);
```

Improper Resource Access Authorization\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3635
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4859	4859

Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4859.         FORC4 fscanf (ifp, "%d", neut+c);
```

Improper Resource Access Authorization\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3636
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5107	5107
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3637
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4831	4831
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4831.        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=1020047&projectid=20040&pathid=3638
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4842	4842
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3639
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4846	4846
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

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

Improper Resource Access Authorization\Path 32:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3640
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4848	4848
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

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

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3641
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4851	4851
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4851.         fscanf (ifp, "%d", &i);
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3642
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4855	4855
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4855.         fscanf (ifp, "%d", &i);
```

Improper Resource Access Authorization\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3643
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4859	4859
Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_mos (int offset)

```
....
4859.         FORC4 fscanf (ifp, "%d", neut+c);
```

Improper Resource Access Authorization\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3644
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5107	5107

Object	fscanf	fscanf

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3645
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	336	336
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method double CLASS getreal (int type)

```
....
336.         u.c[i ^ rev] = fgetc(ifp);
```

Improper Resource Access Authorization\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3646
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	338	338
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method double CLASS getreal (int type)

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

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3647
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	585	585
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method unsigned CLASS getbits (int nbits)

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

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3648
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	586	586
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3649
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	788	788
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS canon_compressed_load_raw()

```
....
788.        c = fgetc(ifp);
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3650
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	898	898
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3651
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1121	1121
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS pentax_tree()

```
....
1121.    FORC(13) bit[1][c] = fgetc(ifp) & 15;
```

Improper Resource Access Authorization\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3652
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1170	1170
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS nikon_compressed_load_raw()

```
....
1170.    ver0 = fgetc(ifp);
```

Improper Resource Access Authorization\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3653
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1171	1171

Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS nikon_compressed_load_raw()

```
....
1171.    ver1 = fgetc(ifp);
```

Improper Resource Access Authorization\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3654
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1246	1246
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS nikon_e995()

```
....
1246.      histo[fgetc(ifp)]++;
```

Improper Resource Access Authorization\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3655
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2416	2416
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2416.       c = fgetc(ifp);
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3656
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2431	2431
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3657
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2432	2432
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2432.       bitbuf += fgetc(ifp);
```

Improper Resource Access Authorization\Path 50:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3658
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2439	2439
Object	fgetc	fgetc

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS kodak_65000_decode (short *out, int bsize)

```
....
2439.       bitbuf += (INT64) fgetc(ifp) << (bits+(j^8));
```

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=1020047&projectid=20040&pathid=4289
Status	New

The NppParameters::load method calls the wcscpy_s function, at line 983 of notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	1008	1008
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1008.                    wcscpy_s(nppDirLocation, _nppPath.c_str());
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4290
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3323 of notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	3350	3350
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3350.                        wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_DELIMITERS], temp.c_str());
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4291
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3323 of notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	3384	3384
Object	wcscpy_s	wcscpy_s

Code Snippet

File Name	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method	void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3384.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_COMMENTS], temp.c_str());
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4292
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3323 of notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	3394	3394
Object	wcscpy_s	wcscpy_s

Code Snippet

File Name	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method	void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3394.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id], kwl);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4293
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3323 of notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	3398	3398

Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3398.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id],
TEXT("imported string too long, needs to be < max_char(30720)"));
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4294
Status New

The NppParameters::stylerStrOp method calls the wcscpy_s function, at line 6682 of notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	6694	6694
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6694.                        wcscpy_s(str, strLen, style._styleDesc);
```

Unchecked Return Value\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4295
Status New

The NppParameters::stylerStrOp method calls the wcscpy_s function, at line 6682 of notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-	notepad-plus-plus@@notepad-plus-plus-

	v7.8.4-CVE-2022-32168-FP.c	v7.8.4-CVE-2022-32168-FP.c
Line	6700	6700
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6700.                                   wcscpy_s(str, strLen2,
style._fontName);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4296
Status	New

The NppParameters::load method calls the wcscpy_s function, at line 983 of notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	1008	1008
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1008.                   wcscpy_s(nppDirLocation, _nppPath.c_str());
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4297
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3343 of notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	3370	3370
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3370.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_DELIMITERS], temp.c_str());
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4298
Status New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3343 of notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	3404	3404
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3404.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_COMMENTS], temp.c_str());
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4299
Status New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3343 of notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	3414	3414
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3414.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id], kwl);
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4300
Status New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3343 of notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	3418	3418
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3418.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id],
TEXT("imported string too long, needs to be < max_char(30720)"));
```

Unchecked Return Value\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4301
Status	New

The NppParameters::stylerStrOp method calls the wcscpy_s function, at line 6746 of notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	6758	6758
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6758.                          wcscpy_s(str, strLen, style._styleDesc);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4302
Status	New

The NppParameters::stylerStrOp method calls the wcscpy_s function, at line 6746 of notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	6764	6764
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6764.                                  wcscpy_s(str, strLen2,
style._fontName);
```

Unchecked Return Value\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4303
Status	New

The NppParameters::load method calls the wcscpy_s function, at line 1004 of notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	1029	1029
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1029.                    wcscpy_s(nppDirLocation, _nppPath.c_str());
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4304
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3366 of notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	3393	3393
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3393.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_DELIMITERS], temp.c_str());
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4305
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3366 of notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	3427	3427
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3427.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_COMMENTS], temp.c_str());
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4306
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3366 of notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	3437	3437
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3437.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id], kwl);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4307
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3366 of notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	3441	3441
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3441.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id],
TEXT("imported string too long, needs to be < max_char(30720)"));
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4308
Status	New

The NppParameters::stylerStrOp method calls the wcscpy_s function, at line 6843 of notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	6855	6855
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6855.                          wcscpy_s(str, strLen, style._styleDesc);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4309
Status	New

The NppParameters::stylerStrOp method calls the wcscpy_s function, at line 6843 of notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	6861	6861
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
6861.                                  wcscpy_s(str, strLen2,
style._fontName);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4310
Status	New

The NppParameters::load method calls the wcscpy_s function, at line 990 of notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	1013	1013

Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1013.                    wcscpy_s(nppDirLocation, _nppPath.c_str());
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4311
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3406 of notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	3433	3433
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3433.                        wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_DELIMITERS], temp.c_str());
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4312
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3406 of notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c

Line	3467	3467
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3467.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_COMMENTS], temp.c_str());
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4313
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3406 of notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	3477	3477
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3477.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id], kwl);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4314
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3406 of notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	3481	3481
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3481.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id],
TEXT("imported string too long, needs to be < max_char(30720)"));
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4315
Status	New

The NppParameters::stylerStrOp method calls the wcscpy_s function, at line 7053 of notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	7065	7065
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
7065.                          wcscpy_s(str, strLen, style._styleDesc);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4316
Status	New

The NppParameters::stylerStrOp method calls the wcscpy_s function, at line 7053 of notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	7071	7071
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
7071.                                   wcscpy_s(str, strLen2,
style._fontName);
```

Unchecked Return Value\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4317
Status New

The NppParameters::load method calls the wcscpy_s function, at line 997 of notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	1020	1020
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1020.                   wcscpy_s(nppDirLocation, _nppPath.c_str());
```

Unchecked Return Value\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4318
Status New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3435 of notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	3462	3462
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3462.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_DELIMITERS], temp.c_str());
```

Unchecked Return Value\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4319
Status New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3435 of notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	3496	3496
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3496.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_COMMENTS], temp.c_str());
```

Unchecked Return Value\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=4320
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3435 of notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	3506	3506
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3506.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id], kwl);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4321
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3435 of notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	3510	3510
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3510.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id],
TEXT("imported string too long, needs to be < max_char(30720)"));
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4322
Status	New

The NppParameters::stylerStrOp method calls the wcscpy_s function, at line 7214 of notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	7226	7226
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
7226.                          wcscpy_s(str, strLen, style._styleDesc);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4323
Status	New

The NppParameters::stylerStrOp method calls the wcscpy_s function, at line 7214 of notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	7232	7232
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method void NppParameters::stylerStrOp(bool op)

```
....
7232.                                  wcscpy_s(str, strLen2,
style._fontName);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4324
Status	New

The NppParameters::load method calls the wcscpy_s function, at line 1002 of notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Line	1025	1025
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1025.                    wcscpy_s(nppDirLocation, _nppPath.c_str());
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4325
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3456 of notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Line	3483	3483
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3483.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_DELIMITERS], temp.c_str());
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4326
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3456 of notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Line	3517	3517
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3517.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_COMMENTS], temp.c_str());
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4327
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3456 of notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Line	3527	3527
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3527.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id], kwl);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4328
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3456 of notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Line	3531	3531
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3531.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id],
TEXT("imported string too long, needs to be < max_char(30720)"));
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4329
Status	New

The NppParameters::load method calls the wcscpy_s function, at line 1005 of notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c

Line	1028	1028
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1028.                    wcscpy_s(nppDirLocation, _nppPath.c_str());
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4330
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3496 of notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Line	3523	3523
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3523.                        wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_DELIMITERS], temp.c_str());
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4331
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3496 of notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Line	3557	3557
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3557.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_COMMENTS], temp.c_str());
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4332
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3496 of notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Line	3567	3567
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3567.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id], kwl);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4333
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3496 of notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Line	3571	3571
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3571.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id],
TEXT("imported string too long, needs to be < max_char(30720)"));
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4334
Status	New

The NppParameters::load method calls the wcscpy_s function, at line 1043 of notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	1066	1066
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method bool NppParameters::load()

```
....
1066.                    wcscpy_s(nppDirLocation, _nppPath.c_str());
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4335
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3551 of notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	3578	3578
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3578.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_DELIMITERS], temp.c_str());
```

Unchecked Return Value\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4336
Status New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3551 of notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	3612	3612
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3612.                          wcscpy_s(_userLangArray[_nbUserLang - 1]-
>_keywordLists[SCE_USER_KWLIST_COMMENTS], temp.c_str());
```

Unchecked Return Value\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=4337
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3551 of notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	3622	3622
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3622.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id], kwl);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4338
Status	New

The NppParameters::feedUserKeywordList method calls the wcscpy_s function, at line 3551 of notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-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	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	3626	3626
Object	wcscpy_s	wcscpy_s

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method void NppParameters::feedUserKeywordList(TiXmlNode *node)

```
....
3626.
      wcscpy_s(_userLangArray[_nbUserLang - 1]->_keywordLists[id],
TEXT("imported string too long, needs to be < max_char(30720)"));
```

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=1020047&projectid=20040&pathid=4128
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	1966	1966
Object	fd	fd

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method int ndpi_load_ipv4_ptree(struct ndpi_detection_module_struct *ndpi_str,

```
....
1966.     fd = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4129
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	2855	2855
Object	fd	fd

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method int ndpi_load_categories_file(struct ndpi_detection_module_struct *ndpi_str,
const char* path) {

```
....
2855.     fd = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4130
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	2917	2917
Object	fd	fd

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method int ndpi_load_protocols_file(struct ndpi_detection_module_struct *ndpi_str, const char* path) {

```
....
2917.    fd = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4131
Status	New

	Source	Destination
File	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Line	245	245
Object	fp	fp

Code Snippet
File Name OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Method static DetectFileHashData *DetectFileHashParse (const DetectEngineCtx *de_ctx,

```
....
245.      fp = fopen(filename, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4132

Status	New

	Source	Destination
File	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Line	253	253
Object	fp	fp

Code Snippet
File Name OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Method static DetectFileHashData *DetectFileHashParse (const DetectEngineCtx *de_ctx,

```
....
253.                    fp = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4133
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.       if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4134
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c

Line	2287	2287
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.      if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4135
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8473	8473
Object	ifp	ifp

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4136
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8659	8659
Object	ofp	ofp

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4137
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3425	3425
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3425.       fp = fopen (fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4138
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3444	3444
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4139
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3482	3482
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS subtract (char *fname)

```
....
3482.    if (!(fp = fopen (fname, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4140
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5512	5512
Object	ifp	ifp

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_external_jpeg()

```
....
5512.      if ((ifp = fopen (jname, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4141
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	7883	7883
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4142
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Line	2140	2140
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4143
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Line	2287	2287

Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4144
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8473	8473
Object	ifp	ifp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4145
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8659	8659
Object	ofp	ofp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4146
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3425	3425
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3425.       fp = fopen (fname, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4147
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3444	3444
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 21:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4148
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3482	3482
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS subtract (char *fname)

```
....
3482.    if (!(fp = fopen (fname, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4149
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5512	5512
Object	ifp	ifp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_external_jpeg()

```
....
5512.      if ((ifp = fopen (jname, "rb"))) {
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4150
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	7883	7883
Object	fp	fp

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4151
Status New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	574	574
Object	f	f

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method unsigned char *stbi_load(char const *filename, int *x, int *y, int *comp, int req_comp)

```
....
574.     FILE *f = fopen(filename, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4152
Status New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	642	642

Object	f	f

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method float *stbi_loadf(char const *filename, int *x, int *y, int *comp, int req_comp)

```
....
642.     FILE *f = fopen(filename, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4153
Status New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	680	680
Object	f	f

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method extern int stbi_is_hdr (char const *filename)

```
....
680.     FILE *f = fopen(filename, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4154
Status New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	4544	4544
Object	f	f

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method int stbi_info(char const *filename, int *x, int *y, int *comp)

```
....
4544.       FILE *f = fopen(filename, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4155
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	1032	1032
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1032.                   ::CreateDirectory(_userPath.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4156
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	1037	1037
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1037.                   ::CreateDirectory(_userPluginConfDir.c_str(),
NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4157
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	1040	1040
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1040.                    ::CreateDirectory(_userPluginConfDir.c_str(),
NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4158
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	1050	1050
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1050.              ::CreateDirectory(nppPluginRootParent.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4159
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	1052	1052
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1052.               ::CreateDirectory(_pluginRootDir.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4160
Status New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	2758	2758
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method void NppParameters::setCloudChoice(const TCHAR *pathChoice)

```
....
2758.               ::CreateDirectory(cloudChoicePath.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4161
Status New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	1032	1032

Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1032.                    ::CreateDirectory(_userPath.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4162
Status New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	1037	1037
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1037.                    ::CreateDirectory(_userPluginConfDir.c_str(),
NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4163
Status New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	1040	1040
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1040.                    ::CreateDirectory(_userPluginConfDir.c_str(),
NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4164
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	1050	1050
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1050.              ::CreateDirectory(nppPluginRootParent.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4165
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	1052	1052
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1052.              ::CreateDirectory(_pluginRootDir.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4166
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	2778	2778
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method void NppParameters::setCloudChoice(const TCHAR *pathChoice)

```
....
2778.             ::CreateDirectory(cloudChoicePath.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4167
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	1053	1053
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1053.                   ::CreateDirectory(_userPath.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4168
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	1058	1058
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1058.                    ::CreateDirectory(_userPluginConfDir.c_str(),
NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4169
Status New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	1061	1061
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1061.                    ::CreateDirectory(_userPluginConfDir.c_str(),
NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4170
Status New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c

Line	1071	1071
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1071.             ::CreateDirectory(nppPluginRootParent.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4171
Status New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	1073	1073
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1073.             ::CreateDirectory(_pluginRootDir.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4172
Status New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	2801	2801
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c

Method	void NppParameters::setCloudChoice(const TCHAR *pathChoice)

```
....
2801.              ::CreateDirectory(cloudChoicePath.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4173
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	1040	1040
Object	CreateDirectory	CreateDirectory

Code Snippet	
File Name	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method	bool NppParameters::load()

```
....
1040.                    ::CreateDirectory(_userPath.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4174
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	1045	1045
Object	CreateDirectory	CreateDirectory

Code Snippet	
File Name	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method	bool NppParameters::load()

```
....
1045.                    ::CreateDirectory(_userPluginConfDir.c_str(),
NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4175
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	1048	1048
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1048.                    ::CreateDirectory(_userPluginConfDir.c_str(),
NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4176
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	1058	1058
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1058.              ::CreateDirectory(nppPluginRootParent.c_str(), NULL);
```

Incorrect Permission Assignment For Critical Resources\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4177

Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	1060	1060
Object	CreateDirectory	CreateDirectory

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1060.             ::CreateDirectory(_pluginRootDir.c_str(), NULL);
```

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=1020047&projectid=20040&pathid=3303
Status	New

The variable declared in null at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 3657 is not initialized when it is used by ip6_hdr at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 3657.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3664	3716
Object	null	ip6_hdr

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method static u_int8_t ndpi_detection_get_l4_internal(struct ndpi_detection_module_struct *ndpi_str,

```
....
3664.     const struct ndpi_ipv6hdr *iph_v6 = NULL;
....
3716.       l4protocol = iph_v6->ip6_hdr.ip6_un1_nxt;
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3304
Status	New

The variable declared in null at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 3657 is not initialized when it is used by ip6_hdr at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 3657.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3664	3713
Object	null	ip6_hdr

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method static u_int8_t ndpi_detection_get_l4_internal(struct ndpi_detection_module_struct *ndpi_str,

```
....
3664.    const struct ndpi_ipv6hdr *iph_v6 = NULL;
....
3713.    else if(iph_v6 != NULL && (l3_len - sizeof(struct
ndpi_ipv6hdr)) >= ntohs(iph_v6->ip6_hdr.ip6_un1_plen)) {
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3305
Status	New

The variable declared in null at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 325 is not initialized when it is used by server at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 325.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	327	380
Object	null	server

Code Snippet
File Name OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Method static int DetectSshSoftwareVersionTestDetect01(void)

```
....
327.      TcpReassemblyThreadCtx *ra_ctx = NULL;
....
380.          FAIL_IF(StreamTcpReassembleAppLayer(&tv, ra_ctx, &ssn,
&ssn.server, p, UPDATE_DIR_PACKET) < 0);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3306
Status	New

The variable declared in null at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 325 is not initialized when it is used by server at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 325.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	327	378
Object	null	server

Code Snippet
File Name OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Method static int DetectSshSoftwareVersionTestDetect01(void)

```
....
327.      TcpReassemblyThreadCtx *ra_ctx = NULL;
....
378.          FAIL_IF(StreamTcpUTAddSegmentWithPayload(&tv, ra_ctx,
&ssn.server, seq, sshbufs[i], sshlens[i]) == -1);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3307
Status	New

The variable declared in null at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 402 is not initialized when it is used by server at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 402.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	404	457
Object	null	server

Code Snippet	
File Name	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Method	static int DetectSshSoftwareVersionTestDetect02(void)

```
....
404.      TcpReassemblyThreadCtx *ra_ctx = NULL;
....
457.          FAIL_IF(StreamTcpReassembleAppLayer(&tv, ra_ctx, &ssn,
&ssn.server, p, UPDATE_DIR_PACKET) < 0);
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3308
Status	New

The variable declared in null at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 402 is not initialized when it is used by server at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 402.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	404	455
Object	null	server

Code Snippet	
File Name	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Method	static int DetectSshSoftwareVersionTestDetect02(void)

```
....
404.      TcpReassemblyThreadCtx *ra_ctx = NULL;
....
455.          FAIL_IF(StreamTcpUTAddSegmentWithPayload(&tv, ra_ctx,
&ssn.server, seq, sshbufs[i], sshlens[i]) == -1);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3309
Status	New

The variable declared in null at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 479 is not initialized when it is used by server at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 479.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-	OISF@@suricata-suricata-7.0.6-CVE-

	2023-35853-FP.c	2023-35853-FP.c
Line	481	534
Object	null	server

Code Snippet
File Name OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Method static int DetectSshSoftwareVersionTestDetect03(void)

```
....
481.      TcpReassemblyThreadCtx *ra_ctx = NULL;
....
534.          FAIL_IF(StreamTcpReassembleAppLayer(&tv, ra_ctx, &ssn,
&ssn.server, p, UPDATE_DIR_PACKET) < 0);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3310
Status	New

The variable declared in null at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 479 is not initialized when it is used by server at OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c in line 479.

	Source	Destination
File	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c	OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Line	481	532
Object	null	server

Code Snippet
File Name OISF@@suricata-suricata-7.0.6-CVE-2023-35853-FP.c
Method static int DetectSshSoftwareVersionTestDetect03(void)

```
....
481.      TcpReassemblyThreadCtx *ra_ctx = NULL;
....
532.          FAIL_IF(StreamTcpUTAddSegmentWithPayload(&tv, ra_ctx,
&ssn.server, seq, sshbufs[i], sshlens[i]) == -1);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3311
Status	New

The variable declared in 0 at nothings@@stb-newest-CVE-2021-3520-FP.c in line 736 is not initialized when it is used by Pointer at nothings@@stb-newest-CVE-2021-3520-FP.c in line 736.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	745	745
Object	0	Pointer

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static void refill_buffer(stbi *s)

```
....
745.        *s->img_buffer = 0;
```

NULL Pointer Dereference\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3312
Status New

The variable declared in 0 at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 3885 is not initialized when it is used by packet_direction at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 3885.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3926	3926
Object	0	packet_direction

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method void ndpi_connection_tracking(struct ndpi_detection_module_struct *ndpi_str,

```
....
3926.       packet->packet_direction = (ntohs(tcph->source) <
ntohs(tcph->dest)) ? 1 : 0;
```

NULL Pointer Dereference\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3313
Status New

The variable declared in 0 at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 3885 is not initialized when it is used by packet_direction at ntop@@nDPI-3.2-CVE-2020-15475-TP.c in line 3885.

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3989	3989
Object	0	packet_direction

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method void ndpi_connection_tracking(struct ndpi_detection_module_struct *ndpi_str,

```
....
3989.       packet->packet_direction = (htons(udph->source) <
htons(udph->dest)) ? 1 : 0;
```

NULL Pointer Dereference\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3314
Status New

The variable declared in 0 at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 83 is not initialized when it is used by bt at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 172.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Line	86	175
Object	0	bt

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Method byte PolynomialMod2::GetByte(size_t n) const

```
....
86.         return 0;
```

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Method void PolynomialMod2::Encode(BufferedTransformation &bt, size_t outputLen) const

```
....
175.              bt.Put(GetByte(i-1));
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3315
Status	New

The variable declared in 0 at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 83 is not initialized when it is used by enc at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 178.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Line	86	182
Object	0	enc

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c

Method byte PolynomialMod2::GetByte(size_t n) const

```
....
86.         return 0;
```

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c

Method void PolynomialMod2::DEREncodeAsOctetString(BufferedTransformation &bt, size_t length) const

```
....
182.        enc.MessageEnd();
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3316
Status	New

The variable declared in 0 at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 98 is not initialized when it is used by r at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 98.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Line	100	101
Object	0	r

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Method PolynomialMod2 PolynomialMod2::Monomial(size_t i)

```
....
100.        PolynomialMod2 r((word)0, i+1);
101.        r.SetBit(i);
```

NULL Pointer Dereference\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3317
Status New

The variable declared in 0 at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 105 is not initialized when it is used by r at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 105.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Line	107	108
Object	0	r

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Method PolynomialMod2 PolynomialMod2::Trinomial(size_t t0, size_t t1, size_t t2)

```
....
107.        PolynomialMod2 r((word)0, t0+1);
108.        r.SetBit(t0);
```

NULL Pointer Dereference\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3318
Status New

The variable declared in 0 at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 105 is not initialized when it is used by r at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 105.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Line	107	109
Object	0	r

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Method PolynomialMod2 PolynomialMod2::Trinomial(size_t t0, size_t t1, size_t t2)

```
....
107.        PolynomialMod2 r((word)0, t0+1);
....
109.        r.SetBit(t1);
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3319
Status	New

The variable declared in 0 at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 105 is not initialized when it is used by r at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 105.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Line	107	110
Object	0	r

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Method PolynomialMod2 PolynomialMod2::Trinomial(size_t t0, size_t t1, size_t t2)

```
....
107.        PolynomialMod2 r((word)0, t0+1);
....
110.        r.SetBit(t2);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3320
Status	New

The variable declared in 0 at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 114 is not initialized when it is used by r at ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c in line 114.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c

Line	116	117
Object	0	r

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2023-50980-TP.c
Method PolynomialMod2 PolynomialMod2::Pentanomial(size_t t0, size_t t1, size_t t2, size_t t3, size_t t4)

```
....
116.        PolynomialMod2 r((word)0, t0+1);
117.        r.SetBit(t0);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3321
Status	New

The variable declared in sm at OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c in line 301 is not initialized when it is used by ctx at OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c in line 301.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	304	316
Object	sm	ctx

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1Setup(DetectEngineCtx *de_ctx, Signature *s, const char *asn1str)

```
....
304.      SigMatch *sm = NULL;
....
316.      sm->ctx = (SigMatchCtx *)ad;
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3322
Status	New

The variable declared in sm at OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c in line 301 is not initialized when it is used by type at OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c in line 301.

	Source	Destination
File	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Line	304	315
Object	sm	type

Code Snippet
File Name OISF@@suricata-suricata-5.0.2-CVE-2023-35853-TP.c
Method static int DetectAsn1Setup(DetectEngineCtx *de_ctx, Signature *s, const char *asn1str)

```
....
304.       SigMatch *sm = NULL;
....
315.       sm->type = DETECT_ASN1;
```

NULL Pointer Dereference\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3323
Status New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1675 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1679	1700
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot02(void)

```
....
1679.      DetectAddress *temp = NULL;
....
1700.      memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3324
Status New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1675 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1679	1703
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot02(void)

```
....
1679.       DetectAddress *temp = NULL;
....
1703.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3325
Status New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1725 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1729	1750
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1729.       DetectAddress *temp = NULL;
....
1750.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3326

Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1725 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1729	1753
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1729.       DetectAddress *temp = NULL;
....
1753.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3327
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1779	1798
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1779.       DetectAddress *temp = NULL;
....
1798.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3328
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1779	1809
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1779.       DetectAddress *temp = NULL;
....
1809.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3329
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1779	1812
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1779.       DetectAddress *temp = NULL;
....
1812.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 28:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3330
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1779	1801
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1779.       DetectAddress *temp = NULL;
....
1801.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3331
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1837	1867
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1837.       DetectAddress *temp = NULL;
....
1867.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3332
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1837	1856
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1837.       DetectAddress *temp = NULL;
....
1856.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3333
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1837	1870
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1837.       DetectAddress *temp = NULL;
....
1870.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3334
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Line	1837	1859
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.7-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1837.       DetectAddress *temp = NULL;
....
1859.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3335
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1675 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1679	1700
Object	temp	ip

Code Snippet

File Name	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method	static int AddressTestIPv6CutNot02(void)

```
....
1679.       DetectAddress *temp = NULL;
....
1700.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3336
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1675 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1679	1703
Object	temp	ip2

Code Snippet

File Name	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method	static int AddressTestIPv6CutNot02(void)

```
....
1679.       DetectAddress *temp = NULL;
....
1703.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3337
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1725 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1729	1750
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1729.       DetectAddress *temp = NULL;
....
1750.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3338
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1725 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1729	1753
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1729.       DetectAddress *temp = NULL;
....
1753.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3339
Status	New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c

Line	1779	1809
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1779.       DetectAddress *temp = NULL;
....
1809.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3340
Status New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1779	1798
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1779.       DetectAddress *temp = NULL;
....
1798.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3341
Status New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775.

	Source	Destination

File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1779	1812
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1779.       DetectAddress *temp = NULL;
....
1812.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3342
Status New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1779	1801
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1779.       DetectAddress *temp = NULL;
....
1801.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3343
Status New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1837	1856
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1837.       DetectAddress *temp = NULL;
....
1856.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3344
Status New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by ip at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1837	1867
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1837.       DetectAddress *temp = NULL;
....
1867.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3345
Status New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1837	1859
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1837.       DetectAddress *temp = NULL;
....
1859.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3346
Status New

The variable declared in temp at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833 is not initialized when it is used by ip2 at OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c in line 1833.

	Source	Destination
File	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c	OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Line	1837	1870
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-5.0.8-CVE-2023-35853-TP.c
Method static int AddressTestIPv6CutNot05(void)

```
....
1837.       DetectAddress *temp = NULL;
....
1870.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3347

Status	New

The variable declared in temp at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1675 is not initialized when it is used by ip at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	1679	1700
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method static int AddressTestIPv6CutNot02(void)

```
....
1679.       DetectAddress *temp = NULL;
....
1700.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3348
Status	New

The variable declared in temp at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1675 is not initialized when it is used by ip2 at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1675.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	1679	1703
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method static int AddressTestIPv6CutNot02(void)

```
....
1679.       DetectAddress *temp = NULL;
....
1703.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 47:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3349
Status	New

The variable declared in temp at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1725 is not initialized when it is used by ip at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	1729	1750
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1729.       DetectAddress *temp = NULL;
....
1750.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3350
Status	New

The variable declared in temp at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1725 is not initialized when it is used by ip2 at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1725.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	1729	1753
Object	temp	ip2

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method static int AddressTestIPv6CutNot03(void)

```
....
1729.       DetectAddress *temp = NULL;
....
1753.       memcpy(&temp->ip2.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3351
Status	New

The variable declared in temp at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1775 is not initialized when it is used by ip at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	1779	1798
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1779.       DetectAddress *temp = NULL;
....
1798.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3352
Status	New

The variable declared in temp at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1775 is not initialized when it is used by ip at OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c in line 1775.

	Source	Destination
File	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Line	1779	1809
Object	temp	ip

Code Snippet
File Name OISF@@suricata-suricata-6.0.0-beta1-CVE-2023-35853-FP.c
Method static int AddressTestIPv6CutNot04(void)

```
....
1779.       DetectAddress *temp = NULL;
....
1809.       memcpy(&temp->ip.address, in6.s6_addr, sizeof(in6.s6_addr));
```

Unchecked Array Index

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unchecked Array Index\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4508
Status	New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	2037	2037
Object	c	c

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static int zbuild_huffman(zhuffman *z, stbi__uint8 *sizelist, int num)

```
....
2037.           z->size[c] = (stbi__uint8)s;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4509
Status	New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c

Line	2038	2038
Object	c	c

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static int zbuild_huffman(zhuffman *z, stbi__uint8 *sizelist, int num)

```
....
2038.           z->value[c] = (stbi__uint16)i;
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4510
Status New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	3403	3403
Object	index1	index1

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static stbi_uc *tga_load(stbi *s, int *x, int *y, int *comp, int req_comp)

```
....
3403.                   tga_data[index1] = tga_data[index2];
```

Unchecked Array Index\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4511
Status New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	3404	3404
Object	index2	index2

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c

Method	static stbi_uc *tga_load(stbi *s, int *x, int *y, int *comp, int req_comp)

```
....
3404.                   tga_data[index2] = temp;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4512
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-11939-TP.c	ntop@@nDPI-3.2-CVE-2020-11939-TP.c
Line	257	257
Object	len	len

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-11939-TP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
257.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4513
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-11939-TP.c	ntop@@nDPI-3.2-CVE-2020-11939-TP.c
Line	275	275
Object	len	len

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-11939-TP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
275.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4514
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-11940-TP.c	ntop@@nDPI-3.2-CVE-2020-11940-TP.c
Line	257	257
Object	len	len

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-11940-TP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
257.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4515
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-11940-TP.c	ntop@@nDPI-3.2-CVE-2020-11940-TP.c
Line	275	275
Object	len	len

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-11940-TP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
275.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4516
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	144	144
Object	len	len

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method char * ndpi_strdup(const char *s)

```
....
144.      m[len] = '\0';
```

Unchecked Array Index\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4517
Status New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	1803	1803
Object	min_buf_len	min_buf_len

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method static int ac_match_handler(AC_MATCH_t *m, AC_TEXT_t *txt, AC_REP_t *match) {

```
....
1803.    buf[min_buf_len] = '\0';
```

Unchecked Array Index\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4518
Status New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	3951	3951
Object	packet_direction	packet_direction

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method void ndpi_connection_tracking(struct ndpi_detection_module_struct *ndpi_str,

```
....
3951.          flow->next_tcp_seq_nr[flow->packet.packet_direction] =
```

Unchecked Array Index\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4519
Status New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	6313	6313
Object	len	len

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method static u_int16_t ndpi_automa_match_string_subprotocol(struct ndpi_detection_module_struct *ndpi_str,

```
....
6313.       m[len] = '\0';
```

Unchecked Array Index\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4520
Status New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	6336	6336
Object	string_to_match_len	string_to_match_len

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method static u_int16_t ndpi_automa_match_string_subprotocol(struct ndpi_detection_module_struct *ndpi_str,

```
....
6336.     string_to_match[string_to_match_len] = '\0';
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4521
Status	New

	Source	Destination
File	ntop@@nDPI-3.4-CVE-2020-11939-FP.c	ntop@@nDPI-3.4-CVE-2020-11939-FP.c
Line	415	415
Object	len	len

Code Snippet
File Name ntop@@nDPI-3.4-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
415.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4522
Status	New

	Source	Destination
File	ntop@@nDPI-3.4-CVE-2020-11939-FP.c	ntop@@nDPI-3.4-CVE-2020-11939-FP.c
Line	435	435
Object	len	len

Code Snippet
File Name ntop@@nDPI-3.4-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
435.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4523

Status	New

	Source	Destination
File	ntop@@nDPI-3.4-CVE-2020-11940-FP.c	ntop@@nDPI-3.4-CVE-2020-11940-FP.c
Line	415	415
Object	len	len

Code Snippet
File Name ntop@@nDPI-3.4-CVE-2020-11940-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
415.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4524
Status	New

	Source	Destination
File	ntop@@nDPI-3.4-CVE-2020-11940-FP.c	ntop@@nDPI-3.4-CVE-2020-11940-FP.c
Line	435	435
Object	len	len

Code Snippet
File Name ntop@@nDPI-3.4-CVE-2020-11940-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
435.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4525
Status	New

	Source	Destination
File	ntop@@nDPI-4.0-CVE-2020-11939-FP.c	ntop@@nDPI-4.0-CVE-2020-11939-FP.c
Line	416	416

Object	len	len

Code Snippet
File Name ntop@@nDPI-4.0-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
416.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4526
Status New

	Source	Destination
File	ntop@@nDPI-4.0-CVE-2020-11939-FP.c	ntop@@nDPI-4.0-CVE-2020-11939-FP.c
Line	436	436
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.0-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
436.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4527
Status New

	Source	Destination
File	ntop@@nDPI-4.0-CVE-2020-11940-FP.c	ntop@@nDPI-4.0-CVE-2020-11940-FP.c
Line	416	416
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.0-CVE-2020-11940-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
416.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4528
Status	New

	Source	Destination
File	ntop@@nDPI-4.0-CVE-2020-11940-FP.c	ntop@@nDPI-4.0-CVE-2020-11940-FP.c
Line	436	436
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.0-CVE-2020-11940-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
436.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4529
Status	New

	Source	Destination
File	ntop@@nDPI-4.2-CVE-2020-11939-FP.c	ntop@@nDPI-4.2-CVE-2020-11939-FP.c
Line	416	416
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.2-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
416.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 23:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4530
Status	New

	Source	Destination
File	ntop@@nDPI-4.2-CVE-2020-11939-FP.c	ntop@@nDPI-4.2-CVE-2020-11939-FP.c
Line	436	436
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.2-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
436.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4531
Status	New

	Source	Destination
File	ntop@@nDPI-4.2-CVE-2020-11940-FP.c	ntop@@nDPI-4.2-CVE-2020-11940-FP.c
Line	416	416
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.2-CVE-2020-11940-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
416.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4532
Status	New

	Source	Destination
File	ntop@@nDPI-4.2-CVE-2020-11940-FP.c	ntop@@nDPI-4.2-CVE-2020-11940-FP.c
Line	436	436
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.2-CVE-2020-11940-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
436.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4533
Status New

	Source	Destination
File	ntop@@nDPI-4.4-CVE-2020-11939-FP.c	ntop@@nDPI-4.4-CVE-2020-11939-FP.c
Line	420	420
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.4-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
420.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4534
Status New

	Source	Destination
File	ntop@@nDPI-4.4-CVE-2020-11939-FP.c	ntop@@nDPI-4.4-CVE-2020-11939-FP.c
Line	440	440
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.4-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
440.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4535
Status	New

	Source	Destination
File	ntop@@nDPI-4.4-CVE-2020-11940-FP.c	ntop@@nDPI-4.4-CVE-2020-11940-FP.c
Line	420	420
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.4-CVE-2020-11940-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
420.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4536
Status	New

	Source	Destination
File	ntop@@nDPI-4.4-CVE-2020-11940-FP.c	ntop@@nDPI-4.4-CVE-2020-11940-FP.c
Line	440	440
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.4-CVE-2020-11940-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
440.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4537
Status	New

	Source	Destination
File	ntop@@nDPI-4.6-CVE-2020-11939-FP.c	ntop@@nDPI-4.6-CVE-2020-11939-FP.c
Line	416	416
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.6-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
416.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4538
Status	New

	Source	Destination
File	ntop@@nDPI-4.6-CVE-2020-11939-FP.c	ntop@@nDPI-4.6-CVE-2020-11939-FP.c
Line	436	436
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.6-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
436.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 32:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4539
Status	New

	Source	Destination
File	ntop@@nDPI-4.6-CVE-2020-11940-FP.c	ntop@@nDPI-4.6-CVE-2020-11940-FP.c
Line	416	416
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.6-CVE-2020-11940-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
416.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4540
Status	New

	Source	Destination
File	ntop@@nDPI-4.6-CVE-2020-11940-FP.c	ntop@@nDPI-4.6-CVE-2020-11940-FP.c
Line	436	436
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.6-CVE-2020-11940-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
436.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4541
Status	New

	Source	Destination
File	ntop@@nDPI-4.8-CVE-2020-11939-FP.c	ntop@@nDPI-4.8-CVE-2020-11939-FP.c
Line	416	416
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.8-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
416.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4542
Status New

	Source	Destination
File	ntop@@nDPI-4.8-CVE-2020-11939-FP.c	ntop@@nDPI-4.8-CVE-2020-11939-FP.c
Line	436	436
Object	len	len

Code Snippet
File Name ntop@@nDPI-4.8-CVE-2020-11939-FP.c
Method static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
436.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4543
Status New

	Source	Destination
File	ntop@@nDPI-4.8-CVE-2020-11940-FP.c	ntop@@nDPI-4.8-CVE-2020-11940-FP.c
Line	416	416
Object	len	len

Code Snippet	
File Name	ntop@@nDPI-4.8-CVE-2020-11940-FP.c
Method	static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
416.        flow->protos.ssh.client_signature[len] = '\0';
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4544
Status	New

	Source	Destination
File	ntop@@nDPI-4.8-CVE-2020-11940-FP.c	ntop@@nDPI-4.8-CVE-2020-11940-FP.c
Line	436	436
Object	len	len

Code Snippet	
File Name	ntop@@nDPI-4.8-CVE-2020-11940-FP.c
Method	static void ndpi_search_ssh_tcp(struct ndpi_detection_module_struct *ndpi_struct, struct ndpi_flow_struct *flow) {

```
....
436.        flow->protos.ssh.server_signature[len] = '\0';
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4545
Status	New

	Source	Destination
File	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Line	66	66
Object	x	x

Code Snippet	
File Name	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Method	int ReadHashString(uint8_t *hash, const char *string, const char *filename, int line_no,

```
....
66.             hash[x] = (uint8_t)value;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4546
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1697	1697
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1697.             rarray[octindex] += rval;
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4547
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1698	1698
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1698.             garray[octindex] += gval;
```

Unchecked Array Index\Path 41:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4548
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1699	1699
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1699.              barray[octindex] += bval;
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4549
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1790	1790
Object	index	index

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1790.       iarray[opop->index] = i + 1;  /* +1 to avoid storing 0 */
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4550
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1821	1821
Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1821.           narray[octindex2] += (l_int32)opop->npix;
```

Unchecked Array Index\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4551
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1822	1822
Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1822.           rarray[octindex2] += (l_int32)opop->npix * rval;
```

Unchecked Array Index\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4552
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1823	1823

Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1823.          garray[octindex2] += (l_int32)opop->npix * gval;
```

Unchecked Array Index\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4553
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1824	1824
Object	octindex2	octindex2

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctreeQuantByPopulation(PIX *pixs,

```
....
1824.          barray[octindex2] += (l_int32)opop->npix * bval;
```

Unchecked Array Index\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4554
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1825	1825
Object	index	index

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4555
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	2400	2400
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2400.          lut1[oqca[nbase + i]->octindex] = nbase + i;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4556
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	2639	2639
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctcubeQuantMixedWithGray(PIX *pixs,

```
....
2639.                  rarray[octindex] += rval;
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4557
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	2640	2640
Object	octindex	octindex

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method pixOctcubeQuantMixedWithGray(PIX *pixs,

```
....
2640.                    garray[octindex] += gval;
```

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=1020047&projectid=20040&pathid=3408
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8432	8432
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3409
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	334	334
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3410
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1958	1958
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3411

Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3926	3926
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3412
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4866	4866
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3413
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Line	7160	7160
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3414
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	7193	7193
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3415
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	7224	7224
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3416
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8193	8193
Object	BinaryExpr	BinaryExpr

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3417
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8432	8432
Object	BinaryExpr	BinaryExpr

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3418
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	334	334
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3419
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	1958	1958
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3420
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3926	3926
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3421
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4866	4866
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3422
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	7160	7160

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3423
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	7193	7193
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3424
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	7224	7224
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3425
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8193	8193
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3426
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	756	756
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3427
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1033	1033
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3428
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1213	1213
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3429
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1465	1465
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3430
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1509	1509
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3431
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1517	1517

Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3432
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	1597	1597
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3433
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2066	2066
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3434
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2087	2087
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3435
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2095	2095
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3436
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2350	2350
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3437
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2489	2489
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3438
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3717	3717
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3439
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3741	3741
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3440
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3825	3825

Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3441
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4074	4074
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3442
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4136	4136
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3443
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4138	4138
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3444
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4204	4204
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3445
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4212	4212
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3446
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4221	4221
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3447
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4222	4222
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3448
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4223	4223
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3449
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4242	4242

Object	<	<

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3450
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4244	4244
Object	<	<

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3451
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4295	4295
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3452
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4407	4407
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3453
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8018	8018
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3454
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	756	756
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3455
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	1033	1033
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3456
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	1213	1213
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3457
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	1465	1465
Object	>	>

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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);
```

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=1020047&projectid=20040&pathid=4479
Status New

	Source	Destination

File	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Line	990	990
Object	sizeof	sizeof

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.4-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
990.        _isx64 = sizeof(void *) == 8;
```

Use of Sizeof On a Pointer Type\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4480
Status New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Line	990	990
Object	sizeof	sizeof

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.8.7-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
990.        _isx64 = sizeof(void *) == 8;
```

Use of Sizeof On a Pointer Type\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4481
Status New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Line	1011	1011
Object	sizeof	sizeof

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1011.       _isx64 = sizeof(void *) == 8;
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4482
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Line	995	995
Object	sizeof	sizeof

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v7.9.3-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
995.        _isx64 = sizeof(void *) == 8;
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4483
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Line	1002	1002
Object	sizeof	sizeof

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1002.       _isx64 = sizeof(void *) == 8;
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4484
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Line	1007	1007
Object	sizeof	sizeof

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.1.6-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1007.       _isx64 = sizeof(void *) == 8;
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4485
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Line	1010	1010
Object	sizeof	sizeof

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.2.1-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1010.       _isx64 = sizeof(void *) == 8;
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4486

Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Line	1048	1048
Object	sizeof	sizeof

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.1-CVE-2022-32168-TP.c
Method bool NppParameters::load()

```
....
1048.        _isx64 = sizeof(void *) == 8;
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4487
Status	New

	Source	Destination
File	notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c	notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c
Line	1050	1050
Object	sizeof	sizeof

Code Snippet
File Name notepad-plus-plus@@notepad-plus-plus-v8.4.5-CVE-2022-32168-FP.c
Method bool NppParameters::load()

```
....
1050.        _isx64 = sizeof(void *) == 8;
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4488
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	616	616

Object	sizeof	sizeof

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method static int init_hyperscan(struct ndpi_detection_module_struct *ndpi_str) {

```
....
616.    expressions = (char**)ndpi_calloc(sizeof(char*), num_patterns +
1);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4489
Status New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	2257	2257
Object	sizeof	sizeof

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method struct ndpi_detection_module_struct *ndpi_init_detection_module(ndpi_init_prefs prefs) {

```
....
2257.    if((sizeof(categories)/sizeof(char*)) !=
NDPI_PROTOCOL_NUM_CATEGORIES) {
```

Use of Sizeof On a Pointer Type\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4490
Status New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	2259	2259
Object	sizeof	sizeof

Code Snippet
File Name ntop@@nDPI-3.2-CVE-2020-15475-TP.c

Method	struct ndpi_detection_module_struct *ndpi_init_detection_module(ndpi_init_prefs prefs) {

```
....
2259.              NDPI_PROTOCOL_NUM_CATEGORIES, (unsigned
int)(sizeof(categories)/sizeof(char*)));
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4491
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	4501	4501
Object	sizeof	sizeof

Code Snippet

File Name	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method	int ndpi_enable_loaded_categories(struct ndpi_detection_module_struct *ndpi_str) {

```
....
4501.      expressions = (const char**)ndpi_calloc(sizeof(char*),
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4492
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c
Line	301	301
Object	sizeof	sizeof

Code Snippet

File Name	ONLYOFFICE@@core-v5.4.99.1786-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 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4493
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c
Line	473	473
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
473.                                  sizeof(CCBORD *) * ccba->nalloc,
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4494
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c
Line	474	474
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
474.                                  2 * sizeof(CCBORD *) * ccba-
>nalloc)) == 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=1020047&projectid=20040&pathid=4495
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1226	1226
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4496
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1230	1230
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=4497
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	2267	2267
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4498
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	2341	2341
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4499
Status	New

	Source	Destination

File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	2375	2375
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4500
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Line	301	301
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4501
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Line	473	473

Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
473.                                    sizeof(CCBORD *) * ccba->nalloc,
```

Use of Sizeof On a Pointer Type\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4502
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Line	474	474
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Method ccbaExtendArray(CCBORDA *ccba)

```
....
474.                                    2 * sizeof(CCBORD *) * ccba-
>nalloc)) == 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=1020047&projectid=20040&pathid=4503
Status New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c
Line	1226	1226
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4504
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c
Line	1230	1230
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4505
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c
Line	2267	2267
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4506
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c
Line	2341	2341
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4507
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c
Line	2375	2375
Object	sizeof	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c
Method pixOctreeQuantNumColors(PIX *pixs,

```
....
2375.       if ((oqca = (OQCELL **)CALLOC(maxcolors, sizeof(OQCELL *)))
== NULL)
```

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=1020047&projectid=20040&pathid=4262
Status	New

The *stbi_load method in nothings@@stb-newest-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	574	574
Object	fopen	fopen

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method unsigned char *stbi_load(char const *filename, int *x, int *y, int *comp, int req_comp)

```
....
574.     FILE *f = fopen(filename, "rb");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4263
Status	New

The *stbi_loadf method in nothings@@stb-newest-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	642	642
Object	fopen	fopen

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method float *stbi_loadf(char const *filename, int *x, int *y, int *comp, int req_comp)

```
....
642.     FILE *f = fopen(filename, "rb");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4264
Status	New

The stbi_is_hdr method in nothings@@stb-newest-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	680	680
Object	fopen	fopen

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method extern int stbi_is_hdr (char const *filename)

```
....
680.     FILE *f = fopen(filename, "rb");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4265
Status	New

The stbi_info method in nothings@@stb-newest-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	4544	4544
Object	fopen	fopen

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c

Method	int stbi_info(char const *filename, int *x, int *y, int *comp)

```
....
4544.       FILE *f = fopen(filename, "rb");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4266
Status	New

The ndpi_load_ipv4_ptree method in ntop@@nDPI-3.2-CVE-2020-15475-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	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	1966	1966
Object	fopen	fopen

Code Snippet	
File Name	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method	int ndpi_load_ipv4_ptree(struct ndpi_detection_module_struct *ndpi_str,

```
....
1966.     fd = fopen(path, "r");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4267
Status	New

The ndpi_load_categories_file method in ntop@@nDPI-3.2-CVE-2020-15475-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	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	2855	2855
Object	fopen	fopen

Code Snippet	
File Name	ntop@@nDPI-3.2-CVE-2020-15475-TP.c

Method	int ndpi_load_categories_file(struct ndpi_detection_module_struct *ndpi_str, const char* path) {

```
....
2855.    fd = fopen(path, "r");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4268
Status	New

The ndpi_load_protocols_file method in ntop@@nDPI-3.2-CVE-2020-15475-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	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	2917	2917
Object	fopen	fopen

Code Snippet	
File Name	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Method	int ndpi_load_protocols_file(struct ndpi_detection_module_struct *ndpi_str, const char* path) {

```
....
2917.    fd = fopen(path, "r");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4269
Status	New

The *DetectFileHashParse method in OISF@@suricata-suricata-6.0.16-CVE-2023-35853-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	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Line	245	245
Object	fopen	fopen

Code Snippet	
File Name	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Method	static DetectFileHashData *DetectFileHashParse (const DetectEngineCtx *de_ctx,

```
....
245.      fp = fopen(filename, "r");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4270
Status	New

The *DetectFileHashParse method in OISF@@suricata-suricata-6.0.16-CVE-2023-35853-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	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Line	253	253
Object	fopen	fopen

Code Snippet	
File Name	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Method	static DetectFileHashData *DetectFileHashParse (const DetectEngineCtx *de_ctx,

```
....
253.                  fp = fopen(path, "r");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4271
Status	New

The ccbaWrite method in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=4272
Status	New

The ccbaRead method in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=4273
Status	New

The main method in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8473	8473

Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8473.       if (!(ifp = fopen (ifname, "rb"))) {
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4274
Status	New

The main method in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8659	8659
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8659.         ofp = fopen (ofname, "wb");
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4275
Status	New

The bad_pixels method in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Line	3425	3425
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3425.       fp = fopen (fname, "r");
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4276
Status	New

The bad_pixels method in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3444	3444
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3444.         if ((fp = fopen (fname, "r"))) break;
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4277
Status	New

The subtract method in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-	ONLYOFFICE@@core-v5.4.99.1786-CVE-

	2022-29776-FP.c	2022-29776-FP.c
Line	3482	3482
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS subtract (char *fname)

```
....
3482.    if (!(fp = fopen (fname, "rb"))) {
```

TOCTOU\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4278
Status New

The parse_external_jpeg method in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5512	5512
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS parse_external_jpeg()

```
....
5512.      if ((ifp = fopen (jname, "rb"))) {
```

TOCTOU\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4279
Status New

The apply_profile method in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	7883	7883
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7883.    else if ((fp = fopen (output, "rb"))) {
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4280
Status	New

The ccbaWrite method in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Line	2140	2140
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Method ccbaWrite(const char *filename,

```
....
2140.      if ((fp = fopen(filename, "wb+")) == NULL)
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4281
Status	New

The ccbaRead method in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2020-36278-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Line	2287	2287
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36278-TP.c
Method ccbaRead(const char *filename)

```
....
2287.       if ((fp = fopen(filename, "rb")) == NULL)
```

TOCTOU\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4282
Status New

The main method in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8473	8473
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8473.       if (!(ifp = fopen (ifname, "rb"))) {
```

TOCTOU\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4283
Status New

The main method in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8659	8659
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

```
....
8659.         ofp = fopen (ofname, "wb");
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4284
Status	New

The bad_pixels method in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3425	3425
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3425.       fp = fopen (fname, "r");
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4285
Status	New

The bad_pixels method in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3444	3444
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS bad_pixels (char *fname)

```
....
3444.         if ((fp = fopen (fname, "r"))) break;
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4286
Status	New

The subtract method in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3482	3482
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS subtract (char *fname)

```
....
3482.     if (!(fp = fopen (fname, "rb"))) {
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4287
Status	New

The parse_external_jpeg method in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5512	5512
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS parse_external_jpeg()

```
....
5512.      if ((ifp = fopen (jname, "rb"))) {
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=4288
Status	New

The apply_profile method in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	7883	7883
Object	fopen	fopen

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS apply_profile (char *input, char *output)

```
....
7883.    else if ((fp = fopen (output, "rb"))) {
```

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=1020047&projectid=20040&pathid=3285
Status	New

The buffer allocated by <= in nothings@@stb-newest-CVE-2021-3520-FP.c at line 2273 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	2276	2276
Object	<=	<=

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static void init_defaults(void)

```
....
2276.     for (i=0; i <= 143; ++i)     default_length[i]   = 8;
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3286
Status	New

The buffer allocated by <= in nothings@@stb-newest-CVE-2021-3520-FP.c at line 2273 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	2281	2281
Object	<=	<=

Code Snippet
File Name nothings@@stb-newest-CVE-2021-3520-FP.c
Method static void init_defaults(void)

```
....
2281.     for (i=0; i <=  31; ++i)     default_distance[i] = 5;
```

Potential Off by One Error in Loops\Path 3:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3287
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3288
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3289
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	983	983
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3290
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	2185	2185
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 7:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3291
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3999	3999
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3292
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4000	4000
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3293
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4258	4258
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3294
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	4289	4289
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20

	040&pathid=3295
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c
Line	1228	1228
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c
Method cqcellTreeCreate(void)

```
....
1228.       for (level = 0; level <= CQ_NLEVELS; level++) {
```

Potential Off by One Error in Loops\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3296
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2020-36281-TP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2020-36281-TP.c
Line	1266	1266
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3297

Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	983	983
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3298
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	2185	2185
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3299
Status	New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3999	3999
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3300
Status New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4000	4000
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3301
Status New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4258	4258
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3302
Status New

The buffer allocated by <= in ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	4289	4289
Object	<=	<=

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method void CLASS median_filter()

```
....
4289.       for (k=0, i = -width; i <= width; i += width)
```

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=1020047&projectid=20040&pathid=3394
Status	New

The size of the buffer used by foveon_thumb in bwide, at line 2803 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	302	2814
Object	str	bwide

Code Snippet

File Name ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Method unsigned CLASS get4()

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

File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3395
Status	New

The size of the buffer used by apply_profile in size, at line 7860 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c

Line	7884	7886
Object	Address	size

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3396
Status New

The size of the buffer used by foveon_thumb in bwide, at line 2803 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	302	2814
Object	str	bwide

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method unsigned CLASS get4()

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

File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20

	040&pathid=3397
Status	New

The size of the buffer used by apply_profile in size, at line 7860 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	7884	7886
Object	Address	size

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3398
Status	New

The size of the buffer used by apply_profile in ntohl, at line 7860 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	7884	7886
Object	Address	ntohl

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3399
Status	New

The size of the buffer used by apply_profile in ntohl, at line 7860 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	7884	7886
Object	Address	ntohl

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3400
Status	New

The size of the buffer used by apply_profile in size, at line 7860 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	7884	7886
Object	Address	size

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3401
Status	New

The size of the buffer used by apply_profile in size, at line 7860 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	7884	7886
Object	Address	size

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=4254
Status	New

The system data read by main in the file ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8455	8455
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=4255
Status New

The system data read by main in the file ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8474	8474
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=4256
Status New

The system data read by main in the file ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8662	8662
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=4257
Status New

The system data read by subtract in the file ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c at line 3476 is potentially exposed by subtract found in ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c at line 3476.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3483	3483
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=4258

Status	New

The system data read by main in the file ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8455	8455
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=4259
Status	New

The system data read by main in the file ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8474	8474
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=4260
Status	New

The system data read by main in the file ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c at line 8313 is potentially exposed by main found in ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c at line 8313.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8662	8662
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=4261
Status	New

The system data read by subtract in the file ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c at line 3476 is potentially exposed by subtract found in ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c at line 3476.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3483	3483
Object	perror	perror

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3402
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-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-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=1020047&projectid=20040&pathid=3403
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-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-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=1020047&projectid=20040&pathid=3404
Status	New

The size of the buffer used by foveon_interpolate in "%sRGBNeutral", at line 3014 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	3074	3074
Object	"%sRGBNeutral"	"%sRGBNeutral"

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3405
Status	New

The size of the buffer used by adobe_coeff in "%s %s", at line 6056 of ONLYOFFICE@@core-v5.4.99.1786-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-v5.4.99.1786-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	6489	6489
Object	"%s %s"	"%s %s"

Code Snippet

File Name	ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3406
Status	New

The size of the buffer used by foveon_interpolate in "%sRGBNeutral", at line 3014 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	3074	3074
Object	"%sRGBNeutral"	"%sRGBNeutral"

Code Snippet

File Name	ONLYOFFICE@@core-v5.5.2.2-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=1020047&projectid=20040&pathid=3407
Status	New

The size of the buffer used by adobe_coeff in "%s %s", at line 6056 of ONLYOFFICE@@core-v5.5.2.2-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-v5.5.2.2-CVE-2022-29776-FP.c, to overwrite the target buffer.

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	6489	6489
Object	"%s %s"	"%s %s"

Code Snippet	
File Name	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method	void CLASS adobe_coeff (char *make, char *model)

```
....
6489.    sprintf (name, "%s %s", make, model);
```

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=1020047&projectid=20040&pathid=3484
Status	New

	Source	Destination
File	nothings@@stb-newest-CVE-2021-3520-FP.c	nothings@@stb-newest-CVE-2021-3520-FP.c
Line	2013	2013
Object	sizes	sizeof

Code Snippet	
File Name	nothings@@stb-newest-CVE-2021-3520-FP.c
Method	static int zbuild_huffman(zhuffman *z, stbi__uint8 *sizelist, int num)

```
....
2013.     memset(sizes, 0, sizeof(sizes));
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3485
Status	New

	Source	Destination
File	ntop@@nDPI-3.2-CVE-2020-15475-TP.c	ntop@@nDPI-3.2-CVE-2020-15475-TP.c
Line	6310	6310
Object	m	sizeof

Code Snippet	
File Name	ntop@@nDPI-3.2-CVE-2020-15475-TP.c

Method	static u_int16_t ndpi_automa_match_string_subprotocol(struct ndpi_detection_module_struct *ndpi_str,

```
....
6310.       int len = ndpi_min(sizeof(m), string_to_match_len);
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3486
Status	New

	Source	Destination
File	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Line	271	271
Object	line	sizeof

Code Snippet	
File Name	OISF@@suricata-suricata-6.0.16-CVE-2023-35853-FP.c
Method	static DetectFileHashData *DetectFileHashParse (const DetectEngineCtx *de_ctx,

```
....
271.       while(fgets(line, (int)sizeof(line), fp) != NULL) {
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3487
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	8588	8588
Object	cmatrix	sizeof

Code Snippet	
File Name	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Method	int CLASS main (int argc, char **argv)

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

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020047&projectid=20040&pathid=3488
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	8588	8588
Object	cmatrix	sizeof

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method int CLASS main (int argc, char **argv)

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

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=1020047&projectid=20040&pathid=3482
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.4.99.1786-CVE-2022-29776-FP.c
Line	5295	5295
Object	tmpfile	tmpfile

Code Snippet
File Name ONLYOFFICE@@core-v5.4.99.1786-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=1020047&projectid=20040&pathid=3483
Status	New

	Source	Destination
File	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c	ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Line	5295	5295
Object	tmpfile	tmpfile

Code Snippet
File Name ONLYOFFICE@@core-v5.5.2.2-CVE-2022-29776-FP.c
Method int CLASS parse_tiff_ifd (int base)

```
....
5295.       if ((ifp = tmpfile())) {
```

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In 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

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 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

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

CGI Stored XSS

Risk

What might happen

Stored malicious data might retrieve system information and exploit the system through CGI (Common Gateway Interface).

Cause

How does it happen

The CGI specification provides opportunities to read files, acquire shell access, and corrupt file systems on server machines and their attached hosts.

Means of gaining access include: exploiting assumptions of the script, exploiting weaknesses in the server environment, and exploiting weaknesses in other programs and system calls.

The primary weakness in CGI scripts is insufficient input validation.

General Recommendations

How to avoid it

Do not provide unnecessary file permissions.

Validate and encode all DB output.

Source Code Examples

Perl

Bad - Printing out data from BD without encoding

```
#!/usr/bin/perl
use CGI;
use DBI;

my $cgi = CGI->new();

$dbh = DBI->connect('dbi:mysql:perltest','root','password')
  or die "Connection Error: $DBI::errstr\n";
$sql = "select * from samples";
$sth = $dbh->prepare($sql);
$sth->execute
  or die "SQL Error: $DBI::errstr\n";

my @row = $sth->fetchrow_array;

print $cgi->header();
      $cgi->start_html(),
      $cgi->p("The result from DB is: ", @row),
      $cgi->end_html;
```

```
```

Good - Printing out from DB after encoding

```
#!/usr/bin/perl
use CGI;
use DBI;
use HTML::Entities;

my $cgi = CGI->new();

$dbh = DBI->connect('dbi:mysql:perltest','root','password')
  or die "Connection Error: $DBI::errstr\n";
$sql = "select * from samples";
$sth = $dbh->prepare($sql);
$sth->execute
  or die "SQL Error: $DBI::errstr\n";

my @row = $sth->fetchrow_array;

print $cgi->header();
      $cgi->start_html(),
      $cgi->p("The result from DB is: ", HTML::Entities::encode(@row)),
      $cgi->end_html;
```

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
```

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;
}
```

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

Off by One Error in Methods

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);
```

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

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;
}
```

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;
}
```

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

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

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

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--;
           }
        }
    }
```

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