

vul_files_88 Scan Report

Project Name	vul_files_88
Scan Start	Thursday, January 9, 2025 2:47:04 PM
Preset	Checkmarx Default
Scan Time	01h:50m:01s
Lines Of Code Scanned	299805
Files Scanned	15
Report Creation Time	Thursday, January 9, 2025 5:12:28 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	8/10000 (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

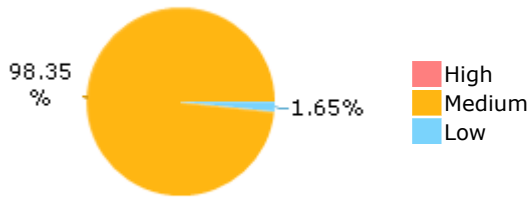
Results Limit

Results limit per query was set to 50

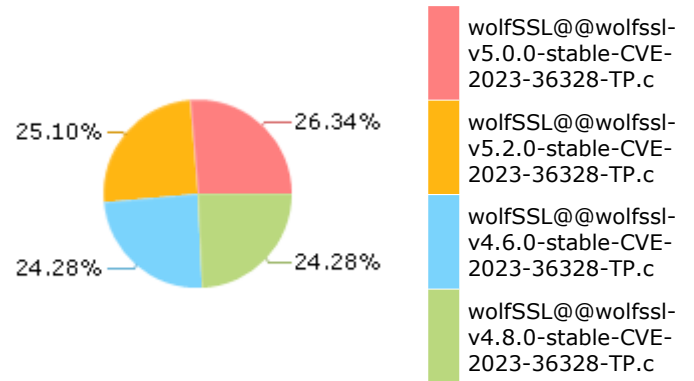
Selected Queries

Selected queries are listed in [Result Summary](#)

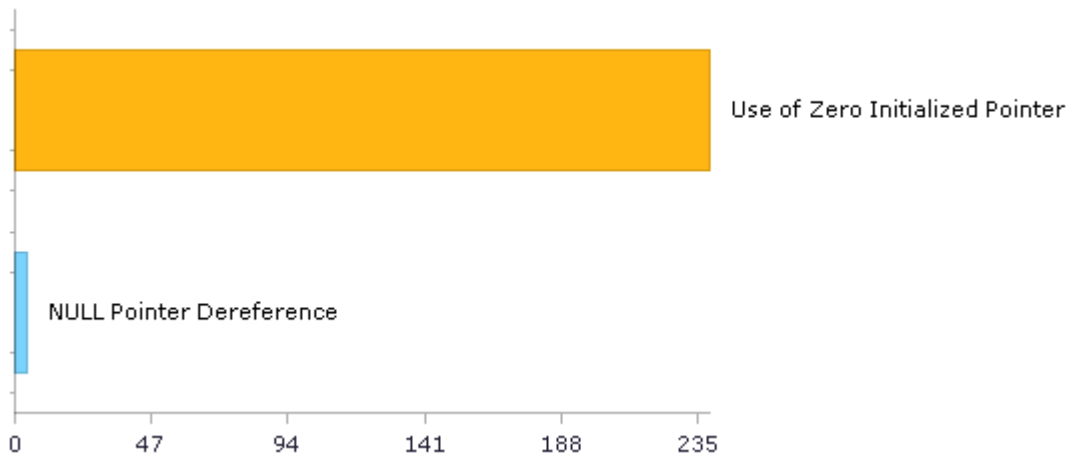
Result Summary



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	4	4
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	0	0
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: [OWASP Top 10 2013](#)

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	0	0
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	0	0
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	0	0
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.	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 - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	0	0
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	243	55
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	0	0
SI-11 Error Handling (P2)*	0	0
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	0	0

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

Scan Summary - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.	0	0
M6-Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	0	0
M8-Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

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

Scan Summary - Custom

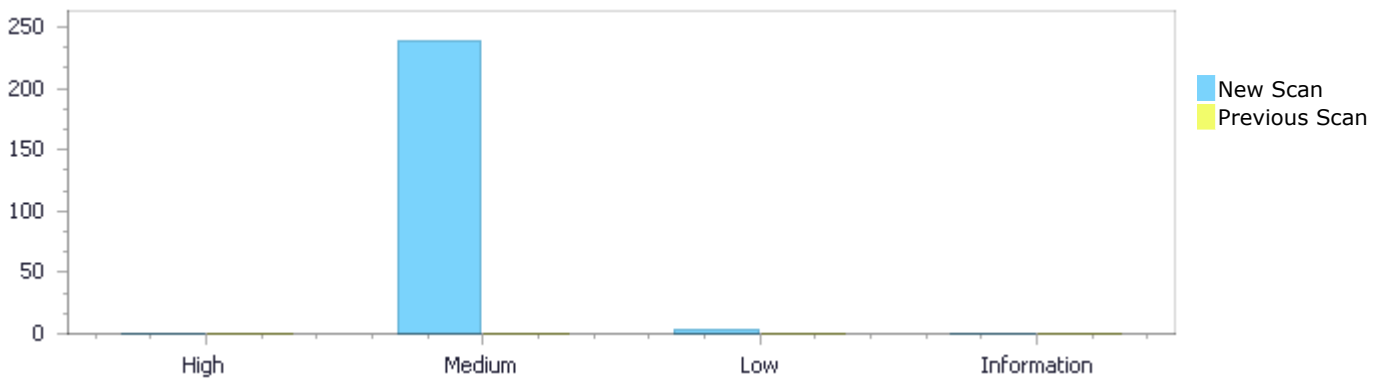
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	0	239	4	0	243
Recurrent Issues	0	0	0	0	0
Total	0	239	4	0	243

Fixed Issues	0	0	0	0	0
--------------	---	---	---	---	---



Results Distribution By State

	High	Medium	Low	Information	Total
Confirmed	0	0	0	0	0
Not Exploitable	0	0	0	0	0
To Verify	0	239	4	0	243
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	239	4	0	243

Result Summary

Vulnerability Type	Occurrences	Severity
Use of Zero Initialized Pointer	239	Medium
NULL Pointer Dereference	4	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
wolfSSL@@wolfssl-v5.0.0-stable-CVE-2023-36328-TP.c	63
wolfSSL@@wolfssl-v5.2.0-stable-CVE-2023-36328-TP.c	60
wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	58
wolfSSL@@wolfssl-v4.8.0-stable-CVE-2023-36328-TP.c	58

Scan Results Details

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=1050093&projectid=50082&pathid=5
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 742.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	798
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_mul_2d (mp_int * a, int b, mp_int * c)

```
....
798.      c->dp[(c->used)++] = r;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=6
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 742.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	798
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....  
207.      a->dp      = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_mul_2d (mp_int * a, int b, mp_int * c)

```
....  
798.      c->dp[ (c->used)++] = r;
```

Use of Zero Initialized Pointer\Path 3:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=7>

Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1661.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	1724
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....  
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int s_mp_add (mp_int * a, mp_int * b, mp_int * c)

```
....
1724.          *tmpc = x->dp[i] + u;
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=8>

Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1661.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	1724
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
207.          a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int s_mp_add (mp_int * a, mp_int * b, mp_int * c)

```
....
1724.          *tmpc = x->dp[i] + u;
```

Use of Zero Initialized Pointer\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=9>

Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1352.

Source	Destination
--------	-------------

File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	1370
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_cmp_mag (mp_int * a, mp_int * b)

```
....
1370.      tmpb = b->dp + (a->used - 1);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=10
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1352.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	1370
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
207.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_cmp_mag (mp_int * a, mp_int * b)

```
.....
1370.      tmpb = b->dp + (a->used - 1);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=11
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1352.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	1367
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
.....
207.      a->dp      = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_cmp_mag (mp_int * a, mp_int * b)

```
.....
1367.      tmpa = a->dp + (a->used - 1);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=12
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1352.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Line	162	1367
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_cmp_mag (mp_int * a, mp_int * b)

```
....
1367.      tmpa = a->dp + (a->used - 1);
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=13>

Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 559.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	589
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
207.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method void mp_rshb (mp_int *c, int x)

```
....
589.      tmpc = c->dp + (c->used - 1);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=14
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 559.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	589
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_rshb (mp_int *c, int x)

```
....
589.      tmpc = c->dp + (c->used - 1);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=15
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 609.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	633
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_rshd (mp_int * a, int b)

```
....
633.      top = a->dp + b;
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=16
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 609.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	633
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_rshd (mp_int * a, int b)

```
....
633.      top = a->dp + b;
```

Use of Zero Initialized Pointer\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=17
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 807.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	833
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_lshd (mp_int * a, int b)

```
....
833.      bottom = a->dp + a->used - 1 - b;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=18
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 807.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	833
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
.....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_lshd (mp_int * a, int b)

```
.....
833.      bottom = a->dp + a->used - 1 - b;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=19
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 807.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	830
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
.....
207.      a->dp      = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_lshd (mp_int * a, int b)

```
.....
830.      top = a->dp + a->used - 1;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=20
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 807.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	830
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_lshd (mp_int * a, int b)

```
....
830.      top = a->dp + a->used - 1;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=21
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 249.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	263
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```


File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_count_bits (mp_int * a)

```
....  
263.      q = a->dp[a->used - 1];
```

Use of Zero Initialized Pointer\Path 18:

Severity Medium
Result State To Verify
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=22>
Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 249.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	263
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....  
207.      a->dp      = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_count_bits (mp_int * a)

```
....  
263.      q = a->dp[a->used - 1];
```

Use of Zero Initialized Pointer\Path 19:

Severity Medium
Result State To Verify
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=23>
Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1563.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	1580
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_div_2(mp_int * a, mp_int * b)

```
....
1580.      tmpa = a->dp + b->used - 1;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=24
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1563.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	1580
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
207.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_div_2(mp_int * a, mp_int * b)

```
.....
1580.         tmpa = a->dp + b->used - 1;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=25
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1563.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	1599
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
.....
162.         a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_div_2(mp_int * a, mp_int * b)

```
.....
1599.         tmpb = b->dp + b->used;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=26
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1563.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Line	207	1599
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_div_2(mp_int * a, mp_int * b)

```
....
1599.      tmpb = b->dp + b->used;
```

Use of Zero Initialized Pointer\Path 23:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=27>

Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1563.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	1583
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_div_2(mp_int * a, mp_int * b)

```
....
1583.      tmpb = b->dp + b->used - 1;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=28
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1563.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	1583
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_div_2(mp_int * a, mp_int * b)

```
....
1583.      tmpb = b->dp + b->used - 1;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=29
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 2881.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	2904
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_set_bit (mp_int * a, int b)

```
....
2904.      a->dp[i] |= ((mp_digit)1) << (b % DIGIT_BIT);
```

Use of Zero Initialized Pointer\Path 26:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=30>

Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 2881.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	2904
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
207.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_set_bit (mp_int * a, int b)

```
....
2904.      a->dp[i] |= ((mp_digit)1) << (b % DIGIT_BIT);
```

Use of Zero Initialized Pointer\Path 27:

Severity Medium

Result State To Verify

Online Results <http://WIN->

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=31
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3195.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	3213
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_div_3 (mp_int * a, mp_int *c, mp_digit * d)

```
....
3213.      w = (w << ((mp_word) DIGIT_BIT)) | ((mp_word) a->dp[ix]);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=32
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3195.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	3213
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_div_3 (mp_int * a, mp_int *c, mp_digit * d)

```
....
3213.      w = (w << ((mp_word)DIGIT_BIT)) | ((mp_word)a->dp[ix]);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=33
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 661.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	689
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_mod_2d (mp_int * a, int b, mp_int * c)

```
....
689.      c->dp[b / DIGIT_BIT] &= ~((mp_digit)0) >> (x +
((sizeof(mp_digit)*8) - DIGIT_BIT));
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=34

Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3568.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	3599
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int s_mp_mul_digs (mp_int * a, mp_int * b, mp_int * c, int digs)

```
....
3599.      tmpx = a->dp[ix];
```

Use of Zero Initialized Pointer\Path 31:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=35>

Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3568.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	3599
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int s_mp_mul_digs (mp_int * a, mp_int * b, mp_int * c, int digs)

```
....
3599.         tmpx = a->dp[ix];
```

Use of Zero Initialized Pointer\Path 32:

Severity Medium
Result State To Verify
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=36>
Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3412.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	3452
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
207.         a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_mul_digs (mp_int * a, mp_int * b, mp_int * c, int digs)

```
....
3452.         tmpx = a->dp + tx;
```

Use of Zero Initialized Pointer\Path 33:

Severity Medium
Result State To Verify
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=37>
Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3412.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	3452
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_mul_digs (mp_int * a, mp_int * b, mp_int * c, int digs)

```
....
3452.      tmpx = a->dp + tx;
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=38
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 4142.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	4212
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_mul_high_digs (mp_int * a, mp_int * b, mp_int * c, int digs)

```
....
4212.      tmpc = c->dp + digs;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=39
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 4142.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	4212
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_mul_high_digs (mp_int * a, mp_int * b, mp_int * c, int digs)

```
....
4212.      tmpc = c->dp + digs;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=40
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 4142.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Line	207	4185
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int fast_s_mp_mul_high_digs (mp_int * a, mp_int * b, mp_int * c, int digs)

```
....
4185.      tmpx = a->dp + tx;
```

Use of Zero Initialized Pointer\Path 37:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=41>

Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 4142.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	4185
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int fast_s_mp_mul_high_digs (mp_int * a, mp_int * b, mp_int * c, int digs)

```
....
4185.      tmpx = a->dp + tx;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=42
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3293.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	3360
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3360.      _W += ((mp_word) a->dp[ix>>1]) * ((mp_word) a->dp[ix>>1]);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=43
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3293.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	3360
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3360.      _W += ((mp_word) a->dp[ix>>1]) * ((mp_word) a->dp[ix>>1]);
```

Use of Zero Initialized Pointer\Path 40:

Severity Medium

Result State To Verify

Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=44>

Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3293.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	3360
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3360.      _W += ((mp_word) a->dp[ix>>1]) * ((mp_word) a->dp[ix>>1]);
```

Use of Zero Initialized Pointer\Path 41:

Severity Medium

Result State To Verify

Online Results <http://WIN->

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=45
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3293.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	3360
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3360.      _W += ((mp_word) a->dp[ix>>1]) * ((mp_word) a->dp[ix>>1]);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=46
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3293.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	3337
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)


```
.....
162.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
.....
3337.      tmpy = a->dp + ty;
```

Use of Zero Initialized Pointer\Path 43:

Severity Medium
Result State To Verify
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=47>
Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3293.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	3337
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
.....
207.      a->dp      = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
.....
3337.      tmpy = a->dp + ty;
```

Use of Zero Initialized Pointer\Path 44:

Severity Medium
Result State To Verify
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=48>
Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3293.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	3336
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....  
162.      a->dp = NULL;
```



File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....  
3336.      tmpx = a->dp + tx;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=49
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3293.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	3336
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....  
207.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int fast_s_mp_sqr (mp_int * a, mp_int * b)

```
....
3336.          tmpx = a->dp + tx;
```

Use of Zero Initialized Pointer\Path 46:

Severity Medium
Result State To Verify
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=50>
Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3501.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	3536
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3536.      r      = ((mp_word) tmpx) * ((mp_word) a->dp[iy]);
```

Use of Zero Initialized Pointer\Path 47:

Severity Medium
Result State To Verify
Online Results <http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=51>
Status New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3501.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	3536
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
....
207.      a->dp      = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3536.      r          = ((mp_word)tmpx) * ((mp_word)a->dp[iy]);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=52
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3501.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	162	3529
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int s_mp_sqr (mp_int * a, mp_int * b)

```
.....
3529.      tmpx      = a->dp[ix];
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=53
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 201 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3501.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	207	3529
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method void mp_free (mp_int * a)

```
.....
207.      a->dp      = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Method int s_mp_sqr (mp_int * a, mp_int * b)

```
.....
3529.      tmpx      = a->dp[ix];
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=54
Status	New

The variable declared in dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 155 is not initialized when it is used by dp at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 3501.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Line	162	3520
Object	dp	dp

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_init (mp_int * a)

```
....
162.      a->dp = NULL;
```

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int s_mp_sqr (mp_int * a, mp_int * b)

```
....
3520.      ((mp_word) a->dp[ix]) * ((mp_word) a->dp[ix]);
```

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=1050093&projectid=50082&pathid=1>

Status New

The variable declared in 0 at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1437 is not initialized when it is used by a at wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c in line 1437.

	Source	Destination
File	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c
Line	1444	1444
Object	0	a

Code Snippet

File Name wolfSSL@@wolfssl-v4.6.0-stable-CVE-2023-36328-TP.c

Method int mp_set (mp_int * a, mp_digit b)

```
....
1444.      a->used = (a->dp[0] != 0) ? 1 : 0;
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=2
Status	New

The variable declared in 0 at wolfSSL@@wolfssl-v4.8.0-stable-CVE-2023-36328-TP.c in line 1435 is not initialized when it is used by a at wolfSSL@@wolfssl-v4.8.0-stable-CVE-2023-36328-TP.c in line 1435.

	Source	Destination
File	wolfSSL@@wolfssl-v4.8.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v4.8.0-stable-CVE-2023-36328-TP.c
Line	1442	1442
Object	0	a

Code Snippet

File Name wolfSSL@@wolfssl-v4.8.0-stable-CVE-2023-36328-TP.c
Method int mp_set (mp_int * a, mp_digit b)

```
....  
1442.      a->used = (a->dp[0] != 0) ? 1 : 0;
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=3
Status	New

The variable declared in 0 at wolfSSL@@wolfssl-v5.0.0-stable-CVE-2023-36328-TP.c in line 1458 is not initialized when it is used by a at wolfSSL@@wolfssl-v5.0.0-stable-CVE-2023-36328-TP.c in line 1458.

	Source	Destination
File	wolfSSL@@wolfssl-v5.0.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.0.0-stable-CVE-2023-36328-TP.c
Line	1465	1465
Object	0	a

Code Snippet

File Name wolfSSL@@wolfssl-v5.0.0-stable-CVE-2023-36328-TP.c
Method int mp_set (mp_int * a, mp_digit b)

```
....  
1465.      a->used = (a->dp[0] != 0) ? 1 : 0;
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1050093&projectid=50082&pathid=4
Status	New

The variable declared in 0 at wolfSSL@@wolfssl-v5.2.0-stable-CVE-2023-36328-TP.c in line 1464 is not initialized when it is used by a at wolfSSL@@wolfssl-v5.2.0-stable-CVE-2023-36328-TP.c in line 1464.

	Source	Destination
File	wolfSSL@@wolfssl-v5.2.0-stable-CVE-2023-36328-TP.c	wolfSSL@@wolfssl-v5.2.0-stable-CVE-2023-36328-TP.c
Line	1471	1471
Object	0	a

Code Snippet

File Name wolfSSL@@wolfssl-v5.2.0-stable-CVE-2023-36328-TP.c
Method int mp_set (mp_int * a, mp_digit b)

```
....  
1471.      a->used = (a->dp[0] != 0) ? 1 : 0;
```

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());
```

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

Scanned Languages

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