# reactos Scan Report

|  |  |
|---|---|
| Project Name | reactos |
| Scan Start | Saturday, June 22, 2024 12:23:40 AM |
| Preset | Checkmarx Default |
| Scan Time | 01h:32m:37s |
| Lines Of Code Scanned | 276050 |
| Files Scanned | 112 |
| Report Creation Time | Saturday, June 22, 2024 12:57:11 AM |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079 |
| Team | CxServer |
| Checkmarx Version | 8.7.0 |
| Scan Type | Full |
| Source Origin | LocalPath |
| Density | 3/10000 (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 |

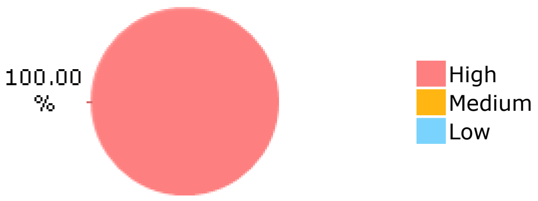
### Results Limit

Results limit per query was set to 50

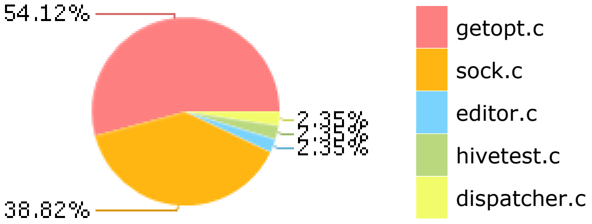
### Selected Queries

Selected queries are listed in Result Summary

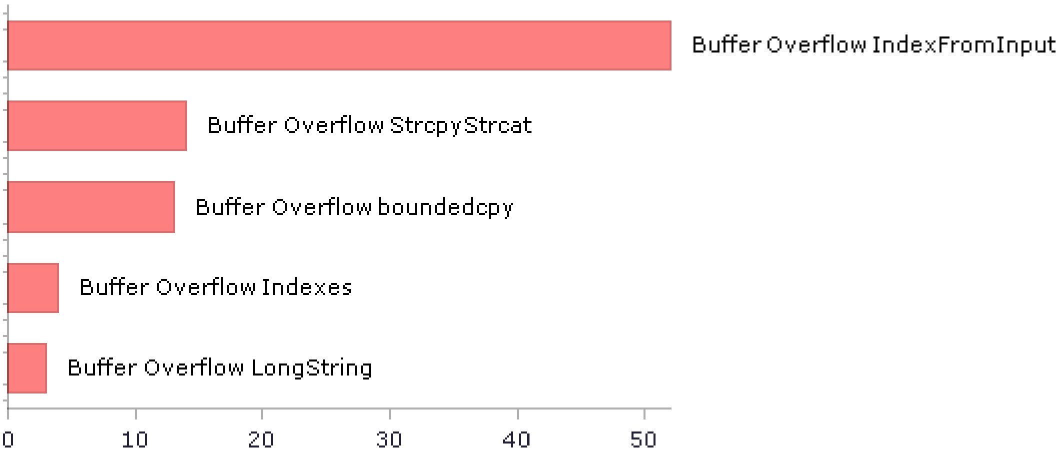
## Result Summary



## 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 | 86 | 14 |
| 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 | 34 | 10 |
| 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)***** | 0 | 0 |
| SC-8 Transmission Confidentiality and Integrity (P1) | 0 | 0 |
| SI-10 Information Input Validation (P1)***** | 34 | 10 |
| 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:<br>-Failing to identify the user at all when that should be required<br>-Failure to maintain the user's identity when it is required<br>-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.).<br>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

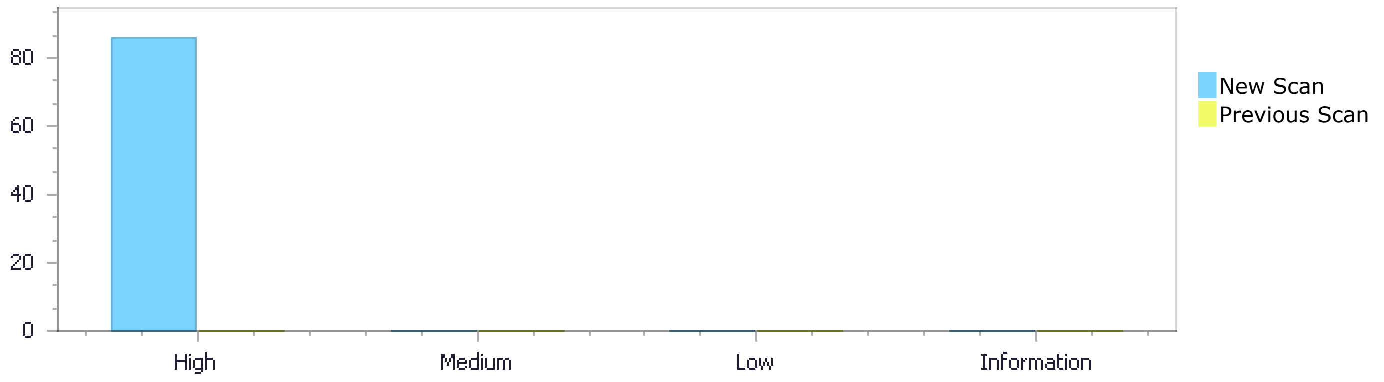
| Category | Issues Found | Best Fix Locations |
|---|---|---|
| Must audit | 0 | 0 |
| Check | 0 | 0 |
| Optional | 0 | 0 |

## Results Distribution By Status

First scan of the project

| | High | Medium | Low | Information | Total |
|---|---|---|---|---|---|
| New Issues | 86 | 0 | 0 | 0 | 86 |
| Recurrent Issues | 0 | 0 | 0 | 0 | 0 |
| Total | 86 | 0 | 0 | 0 | 86 |

| | | | | | |
|---|---|---|---|---|---|
| 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 | 86 | 0 | 0 | 0 | 86 |
| Urgent | 0 | 0 | 0 | 0 | 0 |
| Proposed Not Exploitable | 0 | 0 | 0 | 0 | 0 |
| Total | 86 | 0 | 0 | 0 | 86 |

## Result Summary

| Vulnerability Type | Occurrences | Severity |
|---|---|---|
| Buffer Overflow IndexFromInput | 52 | High |
| Buffer Overflow StrcpyStrcat | 14 | High |
| Buffer Overflow boundedcpy | 13 | High |
| Buffer Overflow Indexes | 4 | High |
| Buffer Overflow LongString | 3 | High |

# 10 Most Vulnerable Files

## High and Medium Vulnerabilities

| File Name | Issues Found |
|---|---|
| reactos/getopt.c | 46 |
| reactos/sock.c | 33 |
| reactos/editor.c | 2 |
| reactos/hivetest.c | 2 |
| reactos/dispatcher.c | 2 |
| reactos/loadlib.c | 1 |

# 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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=21 |
| Status | New |

The size of the buffer used by _getopt_internal_r in PostfixExpr, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 558 |
| Object | argc | PostfixExpr |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

File Name reactos/getopt.c
Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
558.          d->optarg = argv[d->optind++];
```

**Buffer Overflow IndexFromInput\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=22 |
| Status | New |

The size of the buffer used by _getopt_internal_r in PostfixExpr, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 558 |
| Object | argv | PostfixExpr |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

File Name reactos/getopt.c
Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
558.           d->optarg = argv[d->optind++];
```

**Buffer Overflow IndexFromInput\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=23 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 570 |
| Object | argc | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
570.            d->__nextchar = argv[d->optind] + 2;
```

**Buffer Overflow IndexFromInput\Path 4:**

|  |  |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=24 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

|  | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 570 |
| Object | argv | optind |

Code Snippet

File Name reactos/getopt.c

Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
570.            d->__nextchar = argv[d->optind] + 2;
```

**Buffer Overflow IndexFromInput\Path 5:**

|  |  |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=25 |
| Status | New |

The size of the buffer used by process_long_option in optind, at line 191 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

|  | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |

| | | |
|---|---|---|
| Line | 746 | 312 |
| Object | argc | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

File Name reactos/getopt.c

Method process_long_option (int argc, char **argv, const char *optstring,

```
....
312.        if (!long_only || argv[d->optind][1] == '-'
```

### Buffer Overflow IndexFromInput\Path 6:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=26](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=26) |
| Status | New |

The size of the buffer used by process_long_option in optind, at line 191 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 312 |
| Object | argv | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

File Name reactos/getopt.c

Method process_long_option (int argc, char **argv, const char *optstring,

```
....
312.        if (!long_only || argv[d->optind][1] == '-'
```

### Buffer Overflow IndexFromInput\Path 7:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=27 |
| Status | New |

The size of the buffer used by process_long_option in PostfixExpr, at line 191 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 352 |
| Object | argc | PostfixExpr |

Code Snippet

File Name reactos/getopt.c

Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

File Name reactos/getopt.c

Method process_long_option (int argc, char **argv, const char *optstring,

```
....
352.        d->optarg = argv[d->optind++];
```

### Buffer Overflow IndexFromInput\Path 8:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=28 |
| Status | New |

The size of the buffer used by process_long_option in PostfixExpr, at line 191 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 352 |
| Object | argv | PostfixExpr |

Code Snippet

File Name reactos/getopt.c

Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method process_long_option (int argc, char **argv, const char *optstring,

```
....
352.         d->optarg = argv[d->optind++];
```

**Buffer Overflow IndexFromInput\Path 9:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=29 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 644 |
| Object | argc | optind |

Code Snippet

File Name reactos/getopt.c

Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
644.           d->optarg = argv[d->optind];
```

**Buffer Overflow IndexFromInput\Path 10:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=30 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 644 |
| Object | argv | optind |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

▼

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
644.          d->optarg = argv[d->optind];
```

**Buffer Overflow IndexFromInput\Path 11:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=31 |
| Status | New |

The size of the buffer used by _getopt_internal_r in PostfixExpr, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 691 |
| Object | argc | PostfixExpr |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

▼

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
691.              d->optarg = argv[d->optind++];
```

### Buffer Overflow IndexFromInput\Path 12:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=32 |
| Status | New |

The size of the buffer used by _getopt_internal_r in PostfixExpr, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 691 |
| Object | argv | PostfixExpr |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

▼

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
691.              d->optarg = argv[d->optind++];
```

### Buffer Overflow IndexFromInput\Path 13:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=33 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 602 |
| Object | argc | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
602.        d->__nextchar = argv[d->optind] + 1;
```

**Buffer Overflow IndexFromInput\Path 14:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=34 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 602 |
| Object | argv | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
602.        d->__nextchar = argv[d->optind] + 1;
```

### Buffer Overflow IndexFromInput\Path 15:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=35](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=35) |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 592 |
| Object | argc | optind |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

▼

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
592.             d->__nextchar = argv[d->optind] + 1;
```

### Buffer Overflow IndexFromInput\Path 16:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=36](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=36) |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 592 |
| Object | argv | optind |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
592.              d->__nextchar = argv[d->optind] + 1;
```

**Buffer Overflow IndexFromInput\Path 17:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=37 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 588 |
| Object | argc | optind |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
588.           if (long_only && (argv[d->optind][2]
```

**Buffer Overflow IndexFromInput\Path 18:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=38 |

| | |
|---|---|
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 588 |
| Object | argv | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
588.            if (long_only && (argv[d->optind][2]
```

**Buffer Overflow IndexFromInput\Path 19:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=39 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 589 |
| Object | argc | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
589.                    || !strchr (optstring, argv[d->optind][1])))
```

**Buffer Overflow IndexFromInput\Path 20:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=40](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=40) |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 589 |
| Object | argv | optind |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
589.                    || !strchr (optstring, argv[d->optind][1])))
```

**Buffer Overflow IndexFromInput\Path 21:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=41](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=41) |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 566 |
| Object | argc | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
566.           if (argv[d->optind][1] == '-')
```

**Buffer Overflow IndexFromInput\Path 22:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=42 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 566 |
| Object | argv | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
566.           if (argv[d->optind][1] == '-')
```

### Buffer Overflow IndexFromInput\Path 23:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=43 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 554 |
| Object | argc | optind |

Code Snippet

File Name reactos/getopt.c

Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
554.        if (NONOPTION_P)
```

### Buffer Overflow IndexFromInput\Path 24:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=44 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 554 |
| Object | argv | optind |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.   main (int argc, char **argv)
```

▼

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
554.          if (NONOPTION_P)
```

**Buffer Overflow IndexFromInput\Path 25:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=45 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 554 |
| Object | argc | optind |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.   main (int argc, char **argv)
```

▼

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
554.          if (NONOPTION_P)
```

**Buffer Overflow IndexFromInput\Path 26:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=46 |

| | |
|---|---|
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 554 |
| Object | argv | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

File Name reactos/getopt.c
Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
554.         if (NONOPTION_P)
```

### Buffer Overflow IndexFromInput\Path 27:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=47 |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 152 |
| Object | argc | BinaryExpr |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | exchange (char **argv, struct _getopt_data *d) |

```
....
152.                argv[bottom + i] = argv[top - (middle - bottom) + i];
```

**Buffer Overflow IndexFromInput\Path 28:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=48 |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 152 |
| Object | argv | BinaryExpr |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | exchange (char **argv, struct _getopt_data *d) |

```
....
152.                argv[bottom + i] = argv[top - (middle - bottom) + i];
```

**Buffer Overflow IndexFromInput\Path 29:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=49 |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 151 |
| Object | argc | BinaryExpr |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method exchange (char **argv, struct _getopt_data *d)

```
....
151.              tem = argv[bottom + i];
```

**Buffer Overflow IndexFromInput\Path 30:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=50](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=50) |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 151 |
| Object | argv | BinaryExpr |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method exchange (char **argv, struct _getopt_data *d)

```
....
151.              tem = argv[bottom + i];
```

### Buffer Overflow IndexFromInput\Path 31:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=51 |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 168 |
| Object | argc | BinaryExpr |

Code Snippet

File Name reactos/getopt.c

Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

File Name reactos/getopt.c

Method exchange (char **argv, struct _getopt_data *d)

```
....
168.              argv[bottom + i] = argv[middle + i];
```

### Buffer Overflow IndexFromInput\Path 32:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=52 |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 168 |
| Object | argv | BinaryExpr |

Code Snippet

File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method exchange (char **argv, struct _getopt_data *d)

```
....
168.              argv[bottom + i] = argv[middle + i];
```

**Buffer Overflow IndexFromInput\Path 33:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=53](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=53) |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 167 |
| Object | argc | BinaryExpr |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method exchange (char **argv, struct _getopt_data *d)

```
....
167.              tem = argv[bottom + i];
```

**Buffer Overflow IndexFromInput\Path 34:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=54](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=54) |

| | |
|---|---|
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 167 |
| Object | argv | BinaryExpr |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

File Name reactos/getopt.c
Method exchange (char **argv, struct _getopt_data *d)

```
....
167.             tem = argv[bottom + i];
```

**Buffer Overflow IndexFromInput\Path 35:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=55 |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 169 |
| Object | argc | BinaryExpr |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | exchange (char **argv, struct _getopt_data *d) |

```
....
169.                argv[middle + i] = tem;
```

**Buffer Overflow IndexFromInput\Path 36:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=56 |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 169 |
| Object | argv | BinaryExpr |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

▾

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | exchange (char **argv, struct _getopt_data *d) |

```
....
169.                argv[middle + i] = tem;
```

**Buffer Overflow IndexFromInput\Path 37:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=57 |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 168 |
| Object | argc | BinaryExpr |

Code Snippet

File Name reactos/getopt.c

Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

File Name reactos/getopt.c

Method exchange (char **argv, struct _getopt_data *d)

```
....
168.              argv[bottom + i] = argv[middle + i];
```

**Buffer Overflow IndexFromInput\Path 38:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=58 |
| Status | New |

The size of the buffer used by exchange in BinaryExpr, at line 128 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 168 |
| Object | argv | BinaryExpr |

Code Snippet

File Name reactos/getopt.c

Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

File Name reactos/getopt.c

Method exchange (char **argv, struct _getopt_data *d)

```
....
168.              argv[bottom + i] = argv[middle + i];
```

### Buffer Overflow IndexFromInput\Path 39:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=59 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 525 |
| Object | argc | optind |

Code Snippet

File Name reactos/getopt.c

Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
525.        if (d->optind != argc && !strcmp (argv[d->optind], "--"))
```

### Buffer Overflow IndexFromInput\Path 40:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=60 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 525 |
| Object | argv | optind |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

▼

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
525.        if (d->optind != argc && !strcmp (argv[d->optind], "--"))
```

**Buffer Overflow IndexFromInput\Path 41:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=61](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=61) |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 515 |
| Object | argc | optind |

Code Snippet

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | main (int argc, char **argv) |

```
....
746.  main (int argc, char **argv)
```

▼

| | |
|---|---|
| File Name | reactos/getopt.c |
| Method | _getopt_internal_r (int argc, char **argv, const char *optstring, |

```
....
515.          while (d->optind < argc && NONOPTION_P)
```

**Buffer Overflow IndexFromInput\Path 42:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=62](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=62) |

| | |
|---|---|
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 515 |
| Object | argv | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

File Name reactos/getopt.c
Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
515.             while (d->optind < argc && NONOPTION_P)
```

**Buffer Overflow IndexFromInput\Path 43:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=63 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 515 |
| Object | argc | optind |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
515.            while (d->optind < argc && NONOPTION_P)
```

### Buffer Overflow IndexFromInput\Path 44:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=64 |
| Status | New |

The size of the buffer used by _getopt_internal_r in optind, at line 468 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 515 |
| Object | argv | optind |

Code Snippet

File Name reactos/getopt.c

Method main (int argc, char **argv)

```
....
746.  main (int argc, char **argv)
```

▼

File Name reactos/getopt.c

Method _getopt_internal_r (int argc, char **argv, const char *optstring,

```
....
515.            while (d->optind < argc && NONOPTION_P)
```

### Buffer Overflow IndexFromInput\Path 45:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=65 |
| Status | New |

The size of the buffer used by main in PostfixExpr, at line 746 of reactos/getopt.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 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 801 |
| Object | argc | PostfixExpr |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
....
801.          printf ("%s ", argv[optind++]);
```

### Buffer Overflow IndexFromInput\Path 46:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=66 |
| Status | New |

The size of the buffer used by main in PostfixExpr, at line 746 of reactos/getopt.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 argv, at line 746 of reactos/getopt.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/getopt.c | reactos/getopt.c |
| Line | 746 | 801 |
| Object | argv | PostfixExpr |

Code Snippet
File Name reactos/getopt.c
Method main (int argc, char **argv)

```
....
746.   main (int argc, char **argv)
....
801.          printf ("%s ", argv[optind++]);
```

### Buffer Overflow IndexFromInput\Path 47:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=67 |
| Status | New |

The size of the buffer used by LoadLibraryList in len, at line 113 of reactos/loadlib.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 argv, at line 152 of reactos/loadlib.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/loadlib.c | reactos/loadlib.c |
| Line | 152 | 126 |
| Object | argv | len |

Code Snippet
File Name reactos/loadlib.c
Method int __cdecl main(int argc, char* argv[])

```
....
152.  int __cdecl main(int argc, char* argv[])
```

File Name reactos/loadlib.c

Method DWORD LoadLibraryList(char** libnames, int counter, BOOL bUseAnsi)

```
....
126.              libnameW[len] = L'\0';
```

**Buffer Overflow IndexFromInput\Path 48:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=68 |
| Status | New |

The size of the buffer used by select_server in i, at line 740 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that select_server passes to BinaryExpr, at line 740 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 809 | 833 |
| Object | BinaryExpr | i |

Code Snippet
File Name reactos/sock.c
Method static VOID WINAPI select_server ( server_params *par )

```
....
809.                          n_recvd = recv ( mem->sock[i].s, mem-
>sock[i].buf + mem->sock[i].n_recvd, min ( n_expected - mem-
>sock[i].n_recvd, par->buflen ), 0 );
....
833.                          mem->sock[i].n_sent += n_sent;
```

**Buffer Overflow IndexFromInput\Path 49:**

| | |
|---|---|
| Severity | High |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=69 |
| Status | New |

The size of the buffer used by select_server in i, at line 740 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that select_server passes to BinaryExpr, at line 740 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 809 | 811 |
| Object | BinaryExpr | i |

Code Snippet
File Name reactos/sock.c
Method static VOID WINAPI select_server ( server_params *par )

```
....
809.                          n_recvd = recv ( mem->sock[i].s, mem-
>sock[i].buf + mem->sock[i].n_recvd, min ( n_expected - mem-
>sock[i].n_recvd, par->buflen ), 0 );
....
811.                          mem->sock[i].n_recvd += n_recvd;
```

**Buffer Overflow IndexFromInput\Path 50:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=70 |
| Status | New |

The size of the buffer used by select_server in i, at line 740 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that select_server passes to BinaryExpr, at line 740 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 809 | 809 |
| Object | BinaryExpr | i |

Code Snippet
File Name reactos/sock.c
Method static VOID WINAPI select_server ( server_params *par )

```
....
809.                          n_recvd = recv ( mem->sock[i].s, mem-
>sock[i].buf + mem->sock[i].n_recvd, min ( n_expected - mem-
>sock[i].n_recvd, par->buflen ), 0 );
```

## 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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=73 |
| Status | New |

The size of the buffer used by flatten_cmdline in argv, at line 40 of reactos/dispatcher.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that flatten_cmdline passes to argv, at line 40 of reactos/dispatcher.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/dispatcher.c | reactos/dispatcher.c |
| Line | 40 | 67 |
| Object | argv | argv |

Code Snippet
File Name reactos/dispatcher.c
Method char* flatten_cmdline(const char *prog, char* const argv[])

```
....
40.  char* flatten_cmdline(const char *prog, char* const argv[])
....
67.          strcpy(p, argv[i]);
```

**Buffer Overflow StrcpyStrcat\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=74 |
| Status | New |

The size of the buffer used by flatten_cmdline in p, at line 40 of reactos/dispatcher.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that flatten_cmdline passes to argv, at line 40 of reactos/dispatcher.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/dispatcher.c | reactos/dispatcher.c |
| Line | 40 | 67 |
| Object | argv | p |

Code Snippet

| | |
|---|---|
| File Name | reactos/dispatcher.c |
| Method | char* flatten_cmdline(const char *prog, char* const argv[]) |

```
....
40.  char* flatten_cmdline(const char *prog, char* const argv[])
....
67.          strcpy(p, argv[i]);
```

**Buffer Overflow StrcpyStrcat\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=75 |
| Status | New |

The size of the buffer used by get_event_details in name, at line 5533 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5539 |
| Object | name | name |

Code Snippet

| | |
|---|---|
| File Name | reactos/sock.c |
| Method | static void get_event_details(int event, int *bit, char *name) |

```
....
5533.  static void get_event_details(int event, int *bit, char *name)
....
5539.                if (name) strcpy(name, "FD_ACCEPT");
```

**Buffer Overflow StrcpyStrcat\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=76 |
| Status | New |

The size of the buffer used by get_event_details in name, at line 5533 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5543 |

| | | |
|---|---|---|
| Object | name | name |

Code Snippet
File Name reactos/sock.c
Method static void get_event_details(int event, int *bit, char *name)

```
....
5533.   static void get_event_details(int event, int *bit, char *name)
....
5543.                if (name) strcpy(name, "FD_CONNECT");
```

**Buffer Overflow StrcpyStrcat\Path 5:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=77 |
| Status | New |

The size of the buffer used by get_event_details in name, at line 5533 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5547 |
| Object | name | name |

Code Snippet
File Name reactos/sock.c
Method static void get_event_details(int event, int *bit, char *name)

```
....
5533.   static void get_event_details(int event, int *bit, char *name)
....
5547.                if (name) strcpy(name, "FD_READ");
```

**Buffer Overflow StrcpyStrcat\Path 6:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=78 |
| Status | New |

The size of the buffer used by get_event_details in name, at line 5533 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |

|  |  |  |
|---|---|---|
| Line | 5533 | 5551 |
| Object | name | name |

Code Snippet
File Name reactos/sock.c
Method static void get_event_details(int event, int *bit, char *name)

```
....
5533.  static void get_event_details(int event, int *bit, char *name)
....
5551.                 if (name) strcpy(name, "FD_OOB");
```

**Buffer Overflow StrcpyStrcat\Path 7:**

|  |  |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=79 |
| Status | New |

The size of the buffer used by get_event_details in name, at line 5533 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

|  | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5555 |
| Object | name | name |

Code Snippet
File Name reactos/sock.c
Method static void get_event_details(int event, int *bit, char *name)

```
....
5533.  static void get_event_details(int event, int *bit, char *name)
....
5555.                 if (name) strcpy(name, "FD_WRITE");
```

**Buffer Overflow StrcpyStrcat\Path 8:**

|  |  |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=80 |
| Status | New |

The size of the buffer used by get_event_details in name, at line 5533 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

|  | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5559 |
| Object | name | name |

Code Snippet

| | |
|---|---|
| File Name | reactos/sock.c |
| Method | static void get_event_details(int event, int *bit, char *name) |

```
....
5533.   static void get_event_details(int event, int *bit, char *name)
....
5559.               if (name) strcpy(name, "FD_CLOSE");
```

**Buffer Overflow StrcpyStrcat\Path 9:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=81 |
| Status | New |

The size of the buffer used by *dbgstr_event_seq_result in len, at line 5586 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5626 |
| Object | name | len |

Code Snippet

| | |
|---|---|
| File Name | reactos/sock.c |
| Method | static void get_event_details(int event, int *bit, char *name) |

```
....
5533.   static void get_event_details(int event, int *bit, char *name)
```

| | |
|---|---|
| File Name | reactos/sock.c |
| Method | static char *dbgstr_event_seq_result(SOCKET s, WSANETWORKEVENTS *netEvents) |

```
....
5626.       strcpy( message + len, "]" );
```

**Buffer Overflow StrcpyStrcat\Path 10:**

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

| | |
|---|---|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=82 |
| Status | New |

The size of the buffer used by *dbgstr_event_seq_result in BinaryExpr, at line 5586 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5626 |
| Object | name | BinaryExpr |

Code Snippet
File Name reactos/sock.c
Method static void get_event_details(int event, int *bit, char *name)

```
....
5533.   static void get_event_details(int event, int *bit, char *name)
```

File Name reactos/sock.c
Method static char *dbgstr_event_seq_result(SOCKET s, WSANETWORKEVENTS *netEvents)

```
....
5626.       strcpy( message + len, "]" );
```

**Buffer Overflow StrcpyStrcat\Path 11:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=83 |
| Status | New |

The size of the buffer used by *dbgstr_event_seq_result in message, at line 5586 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5626 |
| Object | name | message |

Code Snippet
File Name reactos/sock.c
Method static void get_event_details(int event, int *bit, char *name)

```
....
5533.  static void get_event_details(int event, int *bit, char *name)
```

File Name reactos/sock.c

Method static char *dbgstr_event_seq_result(SOCKET s, WSANETWORKEVENTS *netEvents)

```
....
5626.      strcpy( message + len, "]" );
```

### Buffer Overflow StrcpyStrcat\Path 12:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=84 |
| Status | New |

The size of the buffer used by *dbgstr_event_seq in len, at line 5567 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5582 |
| Object | name | len |

Code Snippet

File Name reactos/sock.c

Method static void get_event_details(int event, int *bit, char *name)

```
....
5533.  static void get_event_details(int event, int *bit, char *name)
```

File Name reactos/sock.c

Method static const char *dbgstr_event_seq(const LPARAM *seq)

```
....
5582.      strcpy( message + len, "]" );
```

### Buffer Overflow StrcpyStrcat\Path 13:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=85 |
| Status | New |

The size of the buffer used by *dbgstr_event_seq in BinaryExpr, at line 5567 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5582 |
| Object | name | BinaryExpr |

Code Snippet

File Name reactos/sock.c

Method static void get_event_details(int event, int *bit, char *name)

```
....
5533.  static void get_event_details(int event, int *bit, char *name)
```

▼

File Name reactos/sock.c

Method static const char *dbgstr_event_seq(const LPARAM *seq)

```
....
5582.      strcpy( message + len, "]" );
```

**Buffer Overflow StrcpyStrcat\Path 14:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | [http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=86](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=86) |
| Status | New |

The size of the buffer used by *dbgstr_event_seq in message, at line 5567 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_event_details passes to name, at line 5533 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 5533 | 5582 |
| Object | name | message |

Code Snippet

File Name reactos/sock.c

Method static void get_event_details(int event, int *bit, char *name)

```
....
5533.  static void get_event_details(int event, int *bit, char *name)
```

▼

| | |
|---|---|
| File Name | reactos/sock.c |
| Method | static const char *dbgstr_event_seq(const LPARAM *seq) |

```
....
5582.        strcpy( message + len, "]" );
```

## Buffer Overflow boundedcpy

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

### Categories

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

*Description*

**Buffer Overflow boundedcpy\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=8 |
| Status | New |

The size parameter BinaryExpr in line 978 in file reactos/editor.c is influenced by the user input url in line 978 in file reactos/editor.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/editor.c | reactos/editor.c |
| Line | 1055 | 1062 |
| Object | url | BinaryExpr |

Code Snippet

| | |
|---|---|
| File Name | reactos/editor.c |
| Method | static INT_PTR CALLBACK hyperlink_dlgproc(HWND hwnd, UINT msg, WPARAM wparam, LPARAM lparam) |

```
....
1055.                      GetWindowTextW(hwndURL, url, len + 1);
....
1062.                      memmove(url + (*type != '\0' ? strlenW(type)
+ 2 : 0), p, (len + 1 - (p - url)) * sizeof(WCHAR));
```

**Buffer Overflow boundedcpy\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=9 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8951 | 9061 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8951.       iret = recv(dest, buf, sizeof(buf), 0);
....
9061.       ok(memcmp(buf, &footer_msg[0], sizeof(footer_msg)) == 0,
```

**Buffer Overflow boundedcpy\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=10 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8961 | 9061 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8961.       iret = recv(dest, buf, sizeof(buf), 0);
....
9061.       ok(memcmp(buf, &footer_msg[0], sizeof(footer_msg)) == 0,
```

**Buffer Overflow boundedcpy\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=500 |

| | |
|---|---|
| | 79&pathid=11 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8982 | 9061 |
| Object | buf | sizeof |

Code Snippet

| | |
|---|---|
| File Name | reactos/sock.c |
| Method | static void test_TransmitFile(void) |

```
....
8982.       iret = recv(dest, buf, sizeof(header_msg), 0);
....
9061.       ok(memcmp(buf, &footer_msg[0], sizeof(footer_msg)) == 0,
```

**Buffer Overflow boundedcpy\Path 5:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=12 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8986 | 9061 |
| Object | buf | sizeof |

Code Snippet

| | |
|---|---|
| File Name | reactos/sock.c |
| Method | static void test_TransmitFile(void) |

```
....
8986.       iret = recv(dest, buf, sizeof(footer_msg), 0);
....
9061.       ok(memcmp(buf, &footer_msg[0], sizeof(footer_msg)) == 0,
```

**Buffer Overflow boundedcpy\Path 6:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=13 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8951 | 9057 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8951.       iret = recv(dest, buf, sizeof(buf), 0);
....
9057.       ok(memcmp(buf, &header_msg[0], sizeof(header_msg)) == 0,
```

**Buffer Overflow boundedcpy\Path 7:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=14 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8961 | 9057 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8961.       iret = recv(dest, buf, sizeof(buf), 0);
....
9057.       ok(memcmp(buf, &header_msg[0], sizeof(header_msg)) == 0,
```

**Buffer Overflow boundedcpy\Path 8:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=15 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8982 | 9057 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8982.       iret = recv(dest, buf, sizeof(header_msg), 0);
....
9057.       ok(memcmp(buf, &header_msg[0], sizeof(header_msg)) == 0,
```

**Buffer Overflow boundedcpy\Path 9:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=16 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8951 | 8987 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8951.       iret = recv(dest, buf, sizeof(buf), 0);
....
8987.       ok(memcmp(buf, &footer_msg[0], sizeof(footer_msg)) == 0,
```

### Buffer Overflow boundedcpy\Path 10:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=17 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8961 | 8987 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8961.       iret = recv(dest, buf, sizeof(buf), 0);
....
8987.       ok(memcmp(buf, &footer_msg[0], sizeof(footer_msg)) == 0,
```

### Buffer Overflow boundedcpy\Path 11:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=18 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8951 | 8983 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8951.       iret = recv(dest, buf, sizeof(buf), 0);
....
8983.       ok(memcmp(buf, &header_msg[0], sizeof(header_msg)) == 0,
```

### Buffer Overflow boundedcpy\Path 12:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=19 |
| Status | New |

The size parameter sizeof in line 8856 in file reactos/sock.c is influenced by the user input buf in line 8856 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8961 | 8983 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8961.       iret = recv(dest, buf, sizeof(buf), 0);
....
8983.       ok(memcmp(buf, &header_msg[0], sizeof(header_msg)) == 0,
```

### Buffer Overflow boundedcpy\Path 13:

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=20 |
| Status | New |

The size parameter sizeof in line 6498 in file reactos/sock.c is influenced by the user input buffer in line 6498 in file reactos/sock.c. This may lead to a buffer overflow vulnerability, which may in turn result in malicious code execution.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 6608 | 6636 |
| Object | buffer | sizeof |

Code Snippet

| | |
|---|---|
| File Name | reactos/sock.c |
| Method | static void test_WSASendMsg(void) |

```
....
6608.       ret = recvfrom(dst, buffer, sizeof(buffer), 0, (struct
sockaddr *) &sockaddr, &addrlen);
....
6636.       memset(buffer, 0, sizeof(buffer));
```

## 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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=4 |
| Status | New |

The size of the buffer used by test_TransmitFile in header_msg, at line 8856 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_TransmitFile passes to buf, at line 8856 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8951 | 8966 |
| Object | buf | header_msg |

Code Snippet

| | |
|---|---|
| File Name | reactos/sock.c |
| Method | static void test_TransmitFile(void) |

```
....
8951.       iret = recv(dest, buf, sizeof(buf), 0);
....
8966.       ok(memcmp(&buf[sizeof(header_msg)], &footer_msg[0],
sizeof(footer_msg)) == 0,
```

**Buffer Overflow Indexes\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=5 |
| Status | New |

The size of the buffer used by test_TransmitFile in sizeof, at line 8856 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_TransmitFile passes to buf, at line 8856 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8951 | 8966 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8951.       iret = recv(dest, buf, sizeof(buf), 0);
....
8966.       ok(memcmp(&buf[sizeof(header_msg)], &footer_msg[0],
sizeof(footer_msg)) == 0,
```

**Buffer Overflow Indexes\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=6 |
| Status | New |

The size of the buffer used by test_TransmitFile in header_msg, at line 8856 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_TransmitFile passes to buf, at line 8856 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8961 | 8966 |
| Object | buf | header_msg |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8961.       iret = recv(dest, buf, sizeof(buf), 0);
....
8966.       ok(memcmp(&buf[sizeof(header_msg)], &footer_msg[0],
sizeof(footer_msg)) == 0,
```

**Buffer Overflow Indexes\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=500 |

| | |
|---|---|
| | 79&pathid=7 |
| Status | New |

The size of the buffer used by test_TransmitFile in sizeof, at line 8856 of reactos/sock.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test_TransmitFile passes to buf, at line 8856 of reactos/sock.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/sock.c | reactos/sock.c |
| Line | 8961 | 8966 |
| Object | buf | sizeof |

Code Snippet
File Name reactos/sock.c
Method static void test_TransmitFile(void)

```
....
8961.       iret = recv(dest, buf, sizeof(buf), 0);
....
8966.       ok(memcmp(&buf[sizeof(header_msg)], &footer_msg[0],
sizeof(footer_msg)) == 0,
```

## 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-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=1 |
| Status | New |

The size of the buffer used by exec_forecolor in color_str, at line 564 of reactos/editor.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that exec_forecolor passes to "#%02x%02x%02x", at line 564 of reactos/editor.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/editor.c | reactos/editor.c |
| Line | 573 | 576 |
| Object | "#%02x%02x%02x" | color_str |

Code Snippet
File Name reactos/editor.c

Method static HRESULT exec_forecolor(HTMLDocument *This, DWORD cmdexecopt, VARIANT *in, VARIANT *out)

```
....
573.              sprintf(color_str, "#%02x%02x%02x",
....
576.              nsICommandParams_SetCStringValue(nsparam,
NSSTATE_ATTRIBUTE, color_str);
```

**Buffer Overflow LongString\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=2 |
| Status | New |

The size of the buffer used by test3 in Buffer, at line 423 of reactos/hivetest.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test3 passes to "\\Registry\\Machine\\Software\\test3reactos", at line 423 of reactos/hivetest.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/hivetest.c | reactos/hivetest.c |
| Line | 433 | 433 |
| Object | "\\Registry\\Machine\\Software\\test3reactos" | Buffer |

Code Snippet
File Name reactos/hivetest.c
Method void test3(void)

```
....
433.    RtlRosInitUnicodeStringFromLiteral(&KeyName,
L"\\Registry\\Machine\\Software\\test3reactos");
```

**Buffer Overflow LongString\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050089&projectid=50079&pathid=3 |
| Status | New |

The size of the buffer used by test3 in Buffer, at line 423 of reactos/hivetest.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that test3 passes to "\\Registry\\Machine\\Software\\test3reactos", at line 423 of reactos/hivetest.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | reactos/hivetest.c | reactos/hivetest.c |
| Line | 446 | 446 |
| Object | "\\Registry\\Machine\\Software\\test3reactos" | Buffer |

Code Snippet
File Name reactos/hivetest.c
Method void test3(void)

```
....
446.    RtlRosInitUnicodeStringFromLiteral(&KeyName,
L"\\Registry\\Machine\\Software\\test3reactos");
```

# 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 boundedcpy

## Risk

### What might happen

Allowing tainted inputs to set the size of how many bytes to copy from source to destination may cause memory corruption, unexpected behavior, instability and data leakage. In some cases, such as when additional and specific areas of memory are also controlled by user input, it may result in code execution.

## Cause

### How does it happen

Should the size of the amount of bytes to copy from source to destination be greater than the size of the destination, an overflow will occur, and memory beyond the intended buffer will get overwritten. Since this size value is derived from user input, the user may provide an invalid and dangerous buffer size.

## General Recommendations

### How to avoid it

- Do not trust memory allocation sizes provided by the user; derive them from the copied values instead.
- If memory allocation by a provided value is absolutely required, restrict this size to safe values only. Specifically ensure that this value does not exceed the destination buffer's size.

## Source Code Examples

### CPP

### Size Parameter is Influenced by User Input

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
strncpy(dest_buf, src_buf, size); //Assuming size is provided by user input
```

### Validating Destination Buffer Length

```
char dest_buf[10];
memset(dest_buf, '\0', sizeof(dest_buf));
if (size < sizeof(dest_buf) && sizeof(src_buf) >= size) //Assuming size is provided by user
input
{
      strncpy(dest_buf, src_buf, size);
}
else
{
      //...
}
```

# Buffer Overflow IndexFromInput

## Risk

### What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

## Cause

### How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

## General Recommendations

### How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

## Source Code Examples

# Buffer Overflow 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

### 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));
    }
}
```

## Scanned Languages

| Language | Hash Number | Change Date |
|---|---|---|
| CPP | 4541647240435660 | 6/19/2024 |
| Common | 0105849645654507 | 6/19/2024 |