

kbengine Scan Report

| | |
|-----------------------|---|
| Project Name | kbengine |
| Scan Start | Friday, June 21, 2024 4:16:21 PM |
| Preset | Checkmarx Default |
| Scan Time | 00h:27m:47s |
| Lines Of Code Scanned | 218751 |
| Files Scanned | 155 |
| Report Creation Time | Friday, June 21, 2024 5:02:24 PM |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033 |
| Team | CxServer |
| Checkmarx Version | 8.7.0 |
| Scan Type | Full |
| Source Origin | LocalPath |
| Density | 1/100 (Vulnerabilities/LOC) |
| Visibility | Public |

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

Uncategorized All

Custom All

PCI DSS v3.2 All

OWASP Top 10 2013 All

FISMA 2014 All

NIST SP 800-53 All

OWASP Top 10 2017 All

OWASP Mobile Top 10
2016 All

Excluded:

Uncategorized None

Custom None

PCI DSS v3.2 None

OWASP Top 10 2013 None

FISMA 2014 None

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

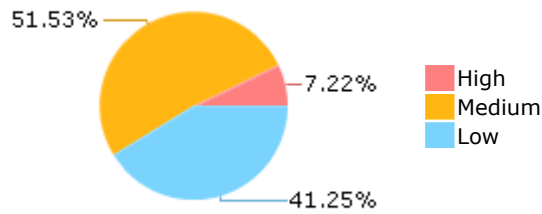
Results Limit

Results limit per query was set to 50

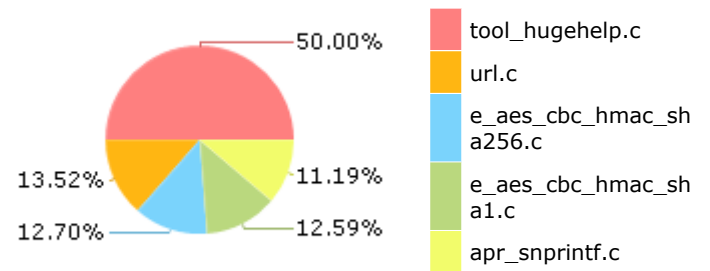
Selected Queries

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

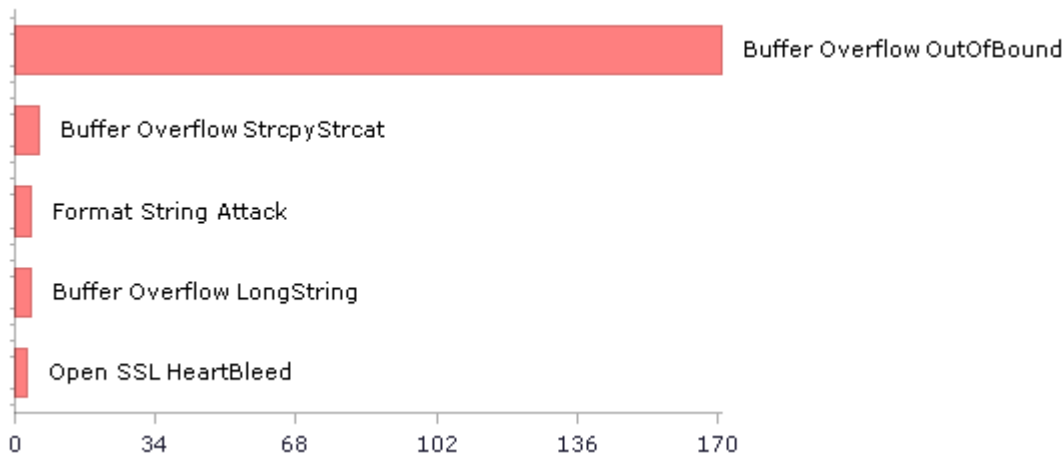
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: [OWASP Top 10 2017](#)

| Category | Threat Agent | Exploitability | Weakness Prevalence | Weakness Detectability | Technical Impact | Business Impact | Issues Found | Best Fix Locations |
|---|---------------|----------------|---------------------|------------------------|------------------|-----------------|--------------|--------------------|
| A1-Injection | App. Specific | EASY | COMMON | EASY | SEVERE | App. Specific | 613 | 301 |
| A2-Broken Authentication | App. Specific | EASY | COMMON | AVERAGE | SEVERE | App. Specific | 591 | 591 |
| A3-Sensitive Data Exposure | App. Specific | AVERAGE | WIDESPREAD | AVERAGE | SEVERE | App. Specific | 17 | 16 |
| 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 | 3 | 1 |
| 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 | 545 | 545 |
| 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 | 2 | 1 |
| 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 | 3 | 1 |
| A6-Sensitive Data Exposure | EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS | DIFFICULT | UNCOMMON | AVERAGE | SEVERE | EXPOSED DATA | 10 | 10 |
| 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 | 545 | 545 |
| 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 | 9 | 9 |
| PCI DSS (3.2) - 6.5.2 - Buffer overflows | 469 | 302 |
| 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. | 10 | 10 |
| 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. | 3 | 3 |
| 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. | 5 | 4 |
| 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. | 595 | 595 |
| 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. | 12 | 12 |
| 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. | 69 | 68 |

* 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) | 592 | 592 |
| 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) | 2 | 2 |
| SC-13 Cryptographic Protection (P1) | 6 | 5 |
| SC-17 Public Key Infrastructure Certificates (P1) | 0 | 0 |
| SC-18 Mobile Code (P2) | 0 | 0 |
| SC-23 Session Authenticity (P1)* | 2 | 2 |
| SC-28 Protection of Information at Rest (P1) | 10 | 10 |
| SC-4 Information in Shared Resources (P1) | 10 | 10 |
| SC-5 Denial of Service Protection (P1)* | 571 | 250 |
| SC-8 Transmission Confidentiality and Integrity (P1) | 0 | 0 |
| SI-10 Information Input Validation (P1)* | 351 | 181 |
| SI-11 Error Handling (P2)* | 70 | 70 |
| SI-15 Information Output Filtering (P0) | 0 | 0 |
| SI-16 Memory Protection (P1) | 14 | 14 |

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

Scan Summary - OWASP Mobile Top 10 2016

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

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

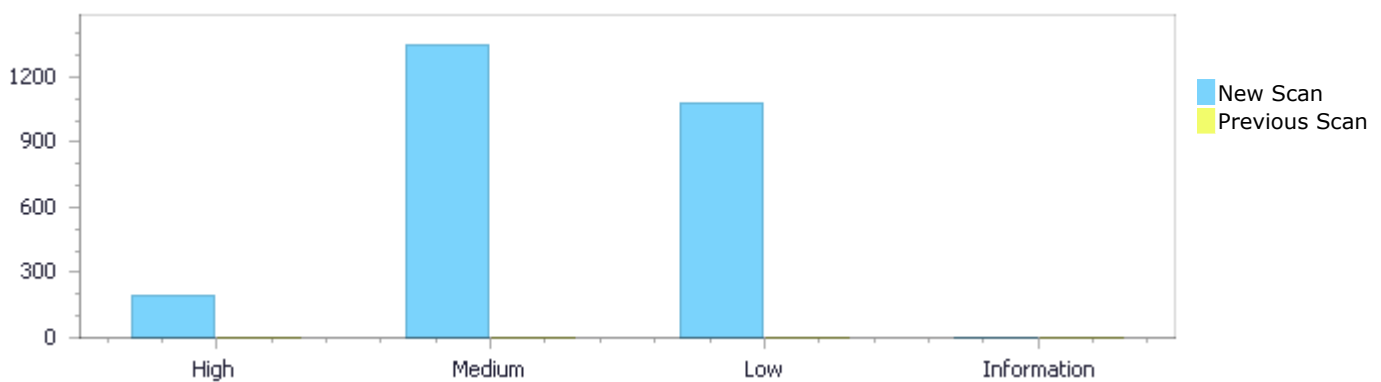
Scan Summary - Custom

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

Results Distribution By Status First scan of the project

| | High | Medium | Low | Information | Total |
|------------------|------|--------|-------|-------------|-------|
| New Issues | 189 | 1,349 | 1,080 | 0 | 2,618 |
| Recurrent Issues | 0 | 0 | 0 | 0 | 0 |
| Total | 189 | 1,349 | 1,080 | 0 | 2,618 |

| | | | | | |
|--------------|---|---|---|---|---|
| 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 | 189 | 1,349 | 1,080 | 0 | 2,618 |
| Urgent | 0 | 0 | 0 | 0 | 0 |
| Proposed Not Exploitable | 0 | 0 | 0 | 0 | 0 |
| Total | 189 | 1,349 | 1,080 | 0 | 2,618 |

Result Summary

| Vulnerability Type | Occurrences | Severity |
|--|-------------|----------|
| Buffer Overflow OutOfBound | 171 | High |
| Buffer Overflow StrcpyStrcat | 6 | High |
| Buffer Overflow LongString | 4 | High |
| Format String Attack | 4 | High |
| Open SSL HeartBleed | 3 | High |

| | | |
|--|-----|--------|
| Buffer Overflow IndexFromInput | 1 | High |
| Dangerous Functions | 545 | Medium |
| Use of Zero Initialized Pointer | 248 | Medium |
| Buffer Overflow boundcpy WrongSizeParam | 211 | Medium |
| Memory Leak | 101 | Medium |
| MemoryFree on StackVariable | 68 | Medium |
| Wrong Size t Allocation | 51 | Medium |
| Integer Overflow | 47 | Medium |
| Long Overflow | 14 | Medium |
| Use of Uninitialized Pointer | 13 | Medium |
| Divide By Zero | 11 | Medium |
| Heap Inspection | 9 | Medium |
| Buffer Overflow AddressOfLocalVarReturned | 5 | Medium |
| Double Free | 5 | Medium |
| Short Overflow | 5 | Medium |
| Inadequate Encryption Strength | 4 | Medium |
| Use of Uninitialized Variable | 4 | Medium |
| Environment Injection | 2 | Medium |
| Use of a One Way Hash without a Salt | 2 | Medium |
| Use of Hard coded Cryptographic Key | 2 | Medium |
| Boolean Overflow | 1 | Medium |
| Char Overflow | 1 | Medium |
| Improper Resource Access Authorization | 581 | Low |
| NULL Pointer Dereference | 197 | Low |
| Unchecked Array Index | 90 | Low |
| Sizeof Pointer Argument | 80 | Low |
| Unchecked Return Value | 70 | Low |
| Use of Sizeof On a Pointer Type | 14 | Low |
| Incorrect Permission Assignment For Critical Resources | 10 | Low |
| Information Exposure Through Comments | 9 | Low |
| Potential Off by One Error in Loops | 9 | Low |
| TOCTOU | 9 | Low |
| Arithmenic Operation On Boolean | 3 | Low |
| Potential Precision Problem | 3 | Low |
| Reliance on DNS Lookups in a Decision | 2 | Low |
| Exposure of System Data to Unauthorized Control Sphere | 1 | Low |
| Privacy Violation | 1 | Low |
| Use of Insufficiently Random Values | 1 | Low |

10 Most Vulnerable Files

High and Medium Vulnerabilities

| File Name | Issues Found |
|----------------------------------|--------------|
| kbengine/e_aes_cbc_hmac_sha256.c | 108 |
| kbengine/e_aes_cbc_hmac_sha1.c | 107 |
| kbengine/url.c | 84 |
| kbengine/multi.c | 82 |
| kbengine/s3_srvr.c | 67 |
| kbengine/http.c | 63 |
| kbengine/s3_clnt.c | 47 |

| | |
|-------------------|----|
| kbengine/ftp.c | 39 |
| kbengine/sds.c | 34 |
| kbengine/cookie.c | 32 |

Scan Results Details

Buffer Overflow OutOfBound

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow OutOfBound 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 OutOfBound\Path 1:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=19 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `out`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 213 | 255 |
| Object | <code>ciph_d</code> | <code>out</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```

....
213.         CIPH_DESC ciph_d[8];
....
255.         ciph_d[i].out = ciph_d[i - 1].out + packlen;

```

Buffer Overflow OutOfBound\Path 2:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=20 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `inp`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 213 | 254 |
| Object | ciph_d | inp |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```

....
213.         CIPH_DESC ciph_d[8];
....
254.         ciph_d[i].inp = hash_d[i].ptr = hash_d[i - 1].ptr + frag;

```

Buffer Overflow OutOfBound\Path 3:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=21>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to ciph_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 213 | 256 |
| Object | ciph_d | ciph_d |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```

....
213.         CIPH_DESC ciph_d[8];
....
256.         memcpy(ciph_d[i].out - 16, IVs, 16);

```

Buffer Overflow OutOfBound\Path 4:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=22>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 213 | 257 |
| Object | ciph_d | ciph_d |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
213.         CIPH_DESC ciph_d[8];  
....  
257.         memcpy(ciph_d[i].iv, IVs, 16);
```

Buffer Overflow OutOfBound\Path 5:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=23>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `blocks`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 213 | 317 |
| Object | ciph_d | blocks |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
213.         CIPH_DESC ciph_d[8];  
....  
317.         ciph_d[i].blocks = MAXCHUNKSIZE / 16;
```

Buffer Overflow OutOfBound\Path 6:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=23>

[33&pathid=24](#)

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `inp`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 213 | 327 |
| Object | ciph_d | inp |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
213.         CIPH_DESC ciph_d[8];  
....  
327.             ciph_d[i].inp += MAXCHUNKSIZE;
```

Buffer Overflow OutOfBound\Path 7:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=25>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `out`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 213 | 328 |
| Object | ciph_d | out |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
213.         CIPH_DESC ciph_d[8];  
....  
328.             ciph_d[i].out += MAXCHUNKSIZE;
```

Buffer Overflow OutOfBound\Path 8:

Severity High

| | |
|----------------|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=26 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in blocks, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 213 | 329 |
| Object | <code>ciph_d</code> | <code>blocks</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```
....  
213.         CIPH_DESC ciph_d[8];  
....  
329.         ciph_d[i].blocks = MAXCHUNKSIZE / 16;
```

Buffer Overflow OutOfBound\Path 9:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=27 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 213 | 330 |
| Object | <code>ciph_d</code> | <code>ciph_d</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```
....  
213.         CIPH_DESC ciph_d[8];  
....  
330.         memcpy(ciph_d[i].iv, ciph_d[i].out - 16, 16);
```

Buffer Overflow OutOfBound\Path 10:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=28 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 213 | 330 |
| Object | <code>ciph_d</code> | <code>ciph_d</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```
....  
213.         CIPH_DESC ciph_d[8];  
....  
330.         memcpy(ciph_d[i].iv, ciph_d[i].out - 16, 16);
```

Buffer Overflow OutOfBound\Path 11:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=29 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 213 | 412 |
| Object | <code>ciph_d</code> | <code>ciph_d</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```
....
213.         CIPH_DESC ciph_d[8];
....
412.         memcpy(ciph_d[i].out, ciph_d[i].inp, len - processed);
```

Buffer Overflow OutOfBound\Path 12:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=30 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 213 | 412 |
| Object | <code>ciph_d</code> | <code>ciph_d</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
 Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```
....
213.         CIPH_DESC ciph_d[8];
....
412.         memcpy(ciph_d[i].out, ciph_d[i].inp, len - processed);
```

Buffer Overflow OutOfBound\Path 13:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=31 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `inp`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 213 | 413 |
| Object | <code>ciph_d</code> | <code>inp</code> |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
213.         CIPH_DESC ciph_d[8];  
....  
413.         ciph_d[i].inp = ciph_d[i].out;
```

Buffer Overflow OutOfBound\Path 14:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=32>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `i`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 213 | 413 |
| Object | ciph_d | i |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
213.         CIPH_DESC ciph_d[8];  
....  
413.         ciph_d[i].inp = ciph_d[i].out;
```

Buffer Overflow OutOfBound\Path 15:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=33>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `blocks`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `ciph_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 213 | 432 |

| | | |
|--------|--------|--------|
| Object | ciph_d | blocks |
|--------|--------|--------|

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```

.....
213.         CIPH_DESC ciph_d[8];
.....
432.         ciph_d[i].blocks = (len - processed) / 16;

```

Buffer Overflow OutOfBound\Path 16:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=34>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 293 |
| Object | hash_d | hash_d |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```

.....
212.         HASH_DESC hash_d[8], edges[8];
.....
293.         memcpy(blocks[i].c + 13, hash_d[i].ptr, 64 - 13);

```

Buffer Overflow OutOfBound\Path 17:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=35>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in ptr, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

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

| | | |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 254 |
| Object | hash_d | ptr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
254.     ciph_d[i].inp = hash_d[i].ptr = hash_d[i - 1].ptr + frag;
```

Buffer Overflow OutOfBound\Path 18:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=36>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in ptr, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 294 |
| Object | hash_d | ptr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
294.     hash_d[i].ptr += 64 - 13;
```

Buffer Overflow OutOfBound\Path 19:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=37>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 295 |
| Object | hash_d | blocks |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
295.     hash_d[i].blocks = (len - (64 - 13)) / 64;
```

Buffer Overflow OutOfBound\Path 20:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=38>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `i`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 315 |
| Object | hash_d | i |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
315.     edges[i].ptr = hash_d[i].ptr;
```

Buffer Overflow OutOfBound\Path 21:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=39>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `ptr`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 324 |
| Object | hash_d | ptr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
324.         edges[i].ptr = hash_d[i].ptr += MAXCHUNKSIZE;
```

Buffer Overflow OutOfBound\Path 22:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=40>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `blocks`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 325 |
| Object | hash_d | blocks |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
325.         hash_d[i].blocks -= MAXCHUNKSIZE / 64;
```

Buffer Overflow OutOfBound\Path 23:

Severity High

Result State To Verify

Online Results <http://WIN->

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=41](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=41)

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `i`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 343 |
| Object | hash_d | i |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
343.         off = hash_d[i].blocks * 64;
```

Buffer Overflow OutOfBound\Path 24:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=42>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `i`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 344 |
| Object | hash_d | i |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
344.         const unsigned char *ptr = hash_d[i].ptr + off;
```

Buffer Overflow OutOfBound\Path 25:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=43 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `q`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 212 | 279 |
| Object | <code>hash_d</code> | <code>q</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
279.     blocks[i].q[0] = BSWAP8(seqnum + i);
```

Buffer Overflow OutOfBound\Path 26:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=44 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `c`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 212 | 286 |
| Object | <code>hash_d</code> | <code>c</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```

....
212.         HASH_DESC hash_d[8], edges[8];
....
286.         blocks[i].c[8] = ((u8 *)key->md.data)[8];

```

Buffer Overflow OutOfBound\Path 27:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=45 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `c`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 212 | 287 |
| Object | <code>hash_d</code> | <code>c</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
 Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```

....
212.         HASH_DESC hash_d[8], edges[8];
....
287.         blocks[i].c[9] = ((u8 *)key->md.data)[9];

```

Buffer Overflow OutOfBound\Path 28:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=46 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `c`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 212 | 288 |
| Object | <code>hash_d</code> | <code>c</code> |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.      HASH_DESC hash_d[8], edges[8];
....
288.      blocks[i].c[10] = ((u8 *)key->md.data)[10];
```

Buffer Overflow OutOfBound\Path 29:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=47>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in c, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 290 |
| Object | hash_d | c |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.      HASH_DESC hash_d[8], edges[8];
....
290.      blocks[i].c[11] = (u8)(len >> 8);
```

Buffer Overflow OutOfBound\Path 30:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=48>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in c, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 291 |

| | | |
|--------|--------|---|
| Object | hash_d | c |
|--------|--------|---|

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
291.     blocks[i].c[12] = (u8) (len);
```

Buffer Overflow OutOfBound\Path 31:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=49 |
| Status | New |

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 293 |
| Object | hash_d | blocks |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
293.     memcpy(blocks[i].c + 13, hash_d[i].ptr, 64 - 13);
```

Buffer Overflow OutOfBound\Path 32:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=50 |
| Status | New |

The size of the buffer used by tls1_1_multi_block_encrypt in i, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

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

| | | |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 297 |
| Object | hash_d | i |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
297.     edges[i].ptr = blocks[i].c;
```

Buffer Overflow OutOfBound\Path 33:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=51>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in blocks, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 347 |
| Object | hash_d | blocks |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
347.     memcpy(blocks[i].c, ptr, off);
```

Buffer Overflow OutOfBound\Path 34:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=52>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in c, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 348 |
| Object | hash_d | c |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.      HASH_DESC hash_d[8], edges[8];  
....  
348.      blocks[i].c[off] = 0x80;
```

Buffer Overflow OutOfBound\Path 35:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=53>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 353 |
| Object | hash_d | d |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.      HASH_DESC hash_d[8], edges[8];  
....  
353.      blocks[i].d[15] = BSWAP4(len);
```

Buffer Overflow OutOfBound\Path 36:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=54>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 360 |
| Object | hash_d | d |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
360.           blocks[i].d[31] = BSWAP4(len);
```

Buffer Overflow OutOfBound\Path 37:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=55>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `i`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 366 |
| Object | hash_d | i |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
366.           edges[i].ptr = blocks[i].c;
```

Buffer Overflow OutOfBound\Path 38:

Severity High

Result State To Verify

Online Results <http://WIN->

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=56](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=56)

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 212 | 375 |
| Object | <code>hash_d</code> | <code>d</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`

Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
375.     blocks[i].d[0] = BSWAP4(ctx->A[i]);
```

Buffer Overflow OutOfBound\Path 39:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=57>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in `d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 212 | 377 |
| Object | <code>hash_d</code> | <code>d</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`

Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
377.     blocks[i].d[1] = BSWAP4(ctx->B[i]);
```

Buffer Overflow OutOfBound\Path 40:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=58 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 212 | 379 |
| Object | <code>hash_d</code> | <code>d</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
379.     blocks[i].d[2] = BSWAP4(ctx->C[i]);
```

Buffer Overflow OutOfBound\Path 41:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=59 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 212 | 381 |
| Object | <code>hash_d</code> | <code>d</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```

....
212.      HASH_DESC hash_d[8], edges[8];
....
381.      blocks[i].d[3] = BSWAP4(ctx->D[i]);

```

Buffer Overflow OutOfBound\Path 42:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=60 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 212 | 383 |
| Object | <code>hash_d</code> | <code>d</code> |

Code Snippet

File Name `kbengine/e_aes_cbc_hmac_sha1.c`
Method `static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,`

```

....
212.      HASH_DESC hash_d[8], edges[8];
....
383.      blocks[i].d[4] = BSWAP4(ctx->E[i]);

```

Buffer Overflow OutOfBound\Path 43:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=61 |
| Status | New |

The size of the buffer used by `tls1_1_multi_block_encrypt` in `c`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|---|---|
| File | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> | <code>kbengine/e_aes_cbc_hmac_sha1.c</code> |
| Line | 212 | 385 |
| Object | <code>hash_d</code> | <code>c</code> |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
385.     blocks[i].c[20] = 0x80;
```

Buffer Overflow OutOfBound\Path 44:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=62>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 386 |
| Object | hash_d | d |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
386.     blocks[i].d[15] = BSWAP4((64 + 20) * 8);
```

Buffer Overflow OutOfBound\Path 45:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=63>

Status New

The size of the buffer used by tls1_1_multi_block_encrypt in i, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 401 |

| | | |
|--------|--------|---|
| Object | hash_d | i |
|--------|--------|---|

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
401.     edges[i].ptr = blocks[i].c;
```

Buffer Overflow OutOfBound\Path 46:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=64 |
| Status | New |

The size of the buffer used by tls1_1_multi_block_encrypt in inp, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 254 |
| Object | hash_d | inp |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
254.     ciph_d[i].inp = hash_d[i].ptr = hash_d[i - 1].ptr + frag;
```

Buffer Overflow OutOfBound\Path 47:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=65 |
| Status | New |

The size of the buffer used by tls1_1_multi_block_encrypt in out, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

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

| | | |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 255 |
| Object | hash_d | out |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
255.     ciph_d[i].out = ciph_d[i - 1].out + packlen;
```

Buffer Overflow OutOfBound\Path 48:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=66 |
| Status | New |

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tls1_1_multi_block_encrypt passes to hash_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 256 |
| Object | hash_d | ciph_d |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
212.     HASH_DESC hash_d[8], edges[8];
....
256.     memcpy(ciph_d[i].out - 16, IVs, 16);
```

Buffer Overflow OutOfBound\Path 49:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=67 |
| Status | New |

The size of the buffer used by tls1_1_multi_block_encrypt in ciph_d, at line 207 of kbengine/e_aes_cbc_hmac_sha1.c, is not properly verified before writing data to the buffer. This can enable a

buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 257 |
| Object | hash_d | ciph_d |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
257.     memcpy(ciph_d[i].iv, IVs, 16);
```

Buffer Overflow OutOfBound\Path 50:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=68>

Status New

The size of the buffer used by `tls1_1_multi_block_encrypt` in blocks, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `tls1_1_multi_block_encrypt` passes to `hash_d`, at line 207 of `kbengine/e_aes_cbc_hmac_sha1.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 212 | 317 |
| Object | hash_d | blocks |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
212.     HASH_DESC hash_d[8], edges[8];  
....  
317.     ciph_d[i].blocks = MAXCHUNKSIZE / 16;
```

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=1030038&projectid=30033&pathid=9 |
| Status | New |

The size of the buffer used by parseurlandfillconn in path, at line 1985 of kbengine/url.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseurlandfillconn passes to path, at line 1985 of kbengine/url.c, to overwrite the target buffer.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 2139 | 2250 |
| Object | path | path |

Code Snippet

File Name kbengine/url.c
Method static CURLcode parseurlandfillconn(struct Curl_easy *data,

```
....  
2139.          protobuf, slashbuf, conn->host.name, path);  
....  
2250.          strcpy(path, "/");
```

Buffer Overflow StrcpyStrcat\Path 2:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=10 |
| Status | New |

The size of the buffer used by parseurlandfillconn in path, at line 1985 of kbengine/url.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseurlandfillconn passes to path, at line 1985 of kbengine/url.c, to overwrite the target buffer.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 2150 | 2250 |
| Object | path | path |

Code Snippet

File Name kbengine/url.c
Method static CURLcode parseurlandfillconn(struct Curl_easy *data,

```
.....
2150.          rc = sscanf(data->change.url, "%[^\n/?#]%[^\n]", conn-
>host.name, path);
.....
2250.          strcpy(path, "/");
```

Buffer Overflow StrcpyStrcat\Path 3:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=11 |
| Status | New |

The size of the buffer used by parseurlandfillconn in path, at line 1985 of kbengine/url.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseurlandfillconn passes to path, at line 1985 of kbengine/url.c, to overwrite the target buffer.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 2062 | 2250 |
| Object | path | path |

Code Snippet

File Name kbengine/url.c
Method static CURLcode parseurlandfillconn(struct Curl_easy *data,

```
.....
2062.          rc = sscanf(data->change.url, "%*15[^\n/:]:%[^\n]", path);
.....
2250.          strcpy(path, "/");
```

Buffer Overflow StrcpyStrcat\Path 4:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=12 |
| Status | New |

The size of the buffer used by parseurlandfillconn in path, at line 1985 of kbengine/url.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseurlandfillconn passes to path, at line 1985 of kbengine/url.c, to overwrite the target buffer.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 2064 | 2250 |
| Object | path | path |

Code Snippet

File Name kbengine/url.c

Method static CURLcode parseurlandfillconn(struct Curl_easy *data,

```
....
2064.         rc = sscanf(data->change.url, "%[^\n]", path);
....
2250.         strcpy(path, "/");
```

Buffer Overflow StrcpyStrcat\Path 5:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=13 |
| Status | New |

The size of the buffer used by *CRYPTO_strdup in ret, at line 364 of kbengine/mem.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *CRYPTO_strdup passes to file, at line 364 of kbengine/mem.c, to overwrite the target buffer.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/mem.c | kbengine/mem.c |
| Line | 364 | 371 |
| Object | file | ret |

Code Snippet

File Name kbengine/mem.c
Method char *CRYPTO_strdup(const char *str, const char *file, int line)

```
....
364. char *CRYPTO_strdup(const char *str, const char *file, int line)
....
371.     strcpy(ret, str);
```

Buffer Overflow StrcpyStrcat\Path 6:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=14 |
| Status | New |

The size of the buffer used by Curl_sec_read_msg in buffer, at line 357 of kbengine/security.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_sec_read_msg passes to buffer, at line 357 of kbengine/security.c, to overwrite the target buffer.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/security.c | kbengine/security.c |
| Line | 357 | 408 |
| Object | buffer | buffer |

Code Snippet

File Name kbengine/security.c
Method int Curl_sec_read_msg(struct connectdata *conn, char *buffer,

```
....
357. int Curl_sec_read_msg(struct connectdata *conn, char *buffer,
....
408. strcpy(buffer, buf);
```

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=1030038&projectid=30033&pathid=1 |
| Status | New |

The size of the buffer used by BF_set_key in tmp, at line 543 of kbengine/crypt_blowfish.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "8b \xd0\xcl\xd2\xcf\xcc\xd8", at line 814 of kbengine/crypt_blowfish.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 817 | 593 |
| Object | "8b \xd0\xcl\xd2\xcf\xcc\xd8" | tmp |

Code Snippet

File Name kbengine/crypt_blowfish.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
817. const char *test_key = "8b \xd0\xcl\xd2\xcf\xcc\xd8";
```



File Name kbengine/crypt_blowfish.c
Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
593. tmp[0] |= (unsigned char)*ptr; /* correct */
```

Buffer Overflow LongString\Path 2:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2 |
| Status | New |

The size of the buffer used by BF_set_key in tmp, at line 543 of kbengine/crypt_blowfish.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "8b \xd0\xcl\xd2\xcf\xcc\xd8", at line 814 of kbengine/crypt_blowfish.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 817 | 595 |
| Object | "8b \xd0\xcl\xd2\xcf\xcc\xd8" | tmp |

Code Snippet

File Name kbengine/crypt_blowfish.c

Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
817.         const char *test_key = "8b \xd0\xcl\xd2\xcf\xcc\xd8";
```



File Name kbengine/crypt_blowfish.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
595.         tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 3:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=3 |
| Status | New |

The size of the buffer used by BF_set_key in tmp, at line 543 of kbengine/crypt_blowfish.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "\xff\xa3", at line 814 of kbengine/crypt_blowfish.c, to overwrite the target buffer.

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 856 | 595 |
| Object | "\xff\xa3" | tmp |

Code Snippet

File Name kbengine/crypt_blowfish.c

Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.          const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```



File Name kbengine/crypt_blowfish.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
595.          tmp[1] |= (BF_word_signed)(signed char)*ptr; /*
bug */
```

Buffer Overflow LongString\Path 4:

Severity High

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=4>

Status New

The size of the buffer used by BF_set_key in tmp, at line 543 of kbengine/crypt_blowfish.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to "\xff\xa3", at line 814 of kbengine/crypt_blowfish.c, to overwrite the target buffer.

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 856 | 593 |
| Object | "\xff\xa3" | tmp |

Code Snippet

File Name kbengine/crypt_blowfish.c

Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....
856.          const char *k = "\xff\xa3" "34" "\xff\xff\xff\xa3"
"345";
```



File Name kbengine/crypt_blowfish.c

Method static void BF_set_key(const char *key, BF_key expanded, BF_key initial,

```
....
593.          tmp[0] |= (unsigned char)*ptr; /* correct */
```

Format String Attack

Query Path:

Categories

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

Description

Format String Attack\Path 1:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=5 |
| Status | New |

Method check_telnet_options at line 818 of kbengine/telnet.c receives the "%127[^=]%*[=]%255s" value from user input. This value is then used to construct a "format string" "%127[^=]%*[=]%255s", which is provided as an argument to a string formatting function in check_telnet_options method of kbengine/telnet.c at line 818.

| | Source | Destination |
|--------|------------------------|------------------------|
| File | kbengine/telnet.c | kbengine/telnet.c |
| Line | 844 | 844 |
| Object | "%127[^=]%*[=]%255s" | "%127[^=]%*[=]%255s" |

Code Snippet

File Name kbengine/telnet.c
 Method static CURLcode check_telnet_options(struct connectdata *conn)

```

....
844.         if(sscanf(head->data, "%127[^= ]%*[ =]%255s",

```

Format String Attack\Path 2:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=6 |
| Status | New |

Method check_telnet_options at line 818 of kbengine/telnet.c receives the "%hu%*[xX]%hu" value from user input. This value is then used to construct a "format string" "%hu%*[xX]%hu", which is provided as an argument to a string formatting function in check_telnet_options method of kbengine/telnet.c at line 818.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/telnet.c | kbengine/telnet.c |
| Line | 877 | 877 |
| Object | "%hu%*[xX]%hu" | "%hu%*[xX]%hu" |

Code Snippet

File Name kbengine/telnet.c

Method static CURLcode check_telnet_options(struct connectdata *conn)

```
....
877.         if(sscanf(option_arg, "%hu%*[xX]%hu",
```

Format String Attack\Path 3:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=7 |
| Status | New |

Method parseurlandfillconn at line 1985 of kbengine/url.c receives the "%*15[^\n/]:%[^\n]" value from user input. This value is then used to construct a "format string" "%*15[^\n/]:%[^\n]", which is provided as an argument to a string formatting function in parseurlandfillconn method of kbengine/url.c at line 1985.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 2062 | 2062 |
| Object | "%*15[^\n/]:%[^\n]" | "%*15[^\n/]:%[^\n]" |

Code Snippet

File Name kbengine/url.c
Method static CURLcode parseurlandfillconn(struct Curl_easy *data,

```
....
2062.         rc = sscanf(data->change.url, "%*15[^\n/]:%[^\n]", path);
```

Format String Attack\Path 4:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=8 |
| Status | New |

Method parse_remote_port at line 3345 of kbengine/url.c receives the "[%*45[0123456789abcdefABCDEF:.]%c" value from user input. This value is then used to construct a "format string" "[%*45[0123456789abcdefABCDEF:.]%c", which is provided as an argument to a string formatting function in parse_remote_port method of kbengine/url.c at line 3345.

| | Source | Destination |
|--------|-------------------------------------|-------------------------------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 3354 | 3354 |
| Object | "[%*45[0123456789abcdefABCDEF:.]%c" | "[%*45[0123456789abcdefABCDEF:.]%c" |

Code Snippet

File Name kbengine/url.c
Method static CURLcode parse_remote_port(struct Curl_easy *data,

```
.....
3354.      if((1 == sscanf(conn->host.name,
"[%*45[0123456789abcdefABCDEF:.]%c",
```

Open SSL HeartBleed

Query Path:

CPP\Cx\CPP Buffer Overflow\Open SSL HeartBleed Version:1

Categories

OWASP Top 10 2013: A5-Security Misconfiguration
 NIST SP 800-53: SI-10 Information Input Validation (P1)
 OWASP Top 10 2017: A6-Security Misconfiguration

Description

Open SSL HeartBleed\Path 1:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=15 |
| Status | New |

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_srvr.c | kbengine/s3_srvr.c |
| Line | 2739 | 2758 |
| Object | i | i |

Code Snippet

File Name kbengine/s3_srvr.c
 Method int ssl3_get_client_key_exchange(SSL *s)

```
.....
2739.      n2s(p, i);
.....
2758.      memcpy(tmp_id, p, i);
```

Open SSL HeartBleed\Path 2:

| | |
|----------------|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=16 |
| Status | New |

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_srvr.c | kbengine/s3_srvr.c |
| Line | 2739 | 1920 |
| Object | i | encodedlen |

Code Snippet

File Name kbengine/s3_srvr.c
Method int ssl3_get_client_key_exchange(SSL *s)

```
....  
2739.          n2s(p, i);
```

File Name kbengine/s3_srvr.c
Method int ssl3_send_server_key_exchange(SSL *s)

```
....  
1920.          (unsigned char *)encodedPoint, encodedlen);
```

Open SSL HeartBleed\Path 3:

Severity High
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=17>
Status New

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_srvr.c | kbengine/s3_srvr.c |
| Line | 2821 | 1920 |
| Object | i | encodedlen |

Code Snippet

File Name kbengine/s3_srvr.c
Method int ssl3_get_client_key_exchange(SSL *s)

```
....  
2821.          n2s(p, i);
```

File Name kbengine/s3_srvr.c
Method int ssl3_send_server_key_exchange(SSL *s)

```
....  
1920.          (unsigned char *)encodedPoint, encodedlen);
```

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=1030038&projectid=30033&pathid=18 |
| Status | New |

The size of the buffer used by decomp in PostfixExpr, at line 282 of kbengine/blast.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 stdin, at line 446 of kbengine/blast.c, to overwrite the target buffer.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/blast.c | kbengine/blast.c |
| Line | 453 | 371 |
| Object | stdin | PostfixExpr |

Code Snippet

File Name kbengine/blast.c
Method int main(void)

```
....
453.      ret = blast(inf, stdin, outf, stdout, &left, NULL);
```



File Name kbengine/blast.c
Method local int decomp(struct state *s)

```
....
371.      s->out[s->next++] = symbol;
```

Dangerous Functions

Query Path:

CPP\Cx\CPP Medium Threat\Dangerous Functions Version:1

Categories

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities

Description

Dangerous Functions\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=619 |
| Status | New |

The dangerous function, _tcslen, was found in use at line 358 in kbengine/schannel.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 401 | 401 |
| Object | _tcslen | _tcslen |

Code Snippet

File Name kbengine/schannel.c

Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
.....
401.      if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=620>

Status New

The dangerous function, _tcslen, was found in use at line 285 in kbengine/schannel_verify.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|----------------------------|----------------------------|
| File | kbengine/schannel_verify.c | kbengine/schannel_verify.c |
| Line | 378 | 378 |
| Object | _tcslen | _tcslen |

Code Snippet

File Name kbengine/schannel_verify.c

Method static CURLcode verify_host(struct Curl_easy *data,

```
.....
378.      cert_hostname_len = _tcslen(
```

Dangerous Functions\Path 3:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=621>

Status New

The dangerous function, memcpy, was found in use at line 213 in kbengine/_ctypes_test.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |

| | | |
|--------|--------|--------|
| Line | 219 | 219 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/_ctypes_test.c
Method EXPORT(wchar_t *) my_wcsdup(wchar_t *src)

```
....
219.      memcpy(ptr, src, (len+1) * sizeof(wchar_t));
```

Dangerous Functions\Path 4:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=622 |
| Status | New |

The dangerous function, memcpy, was found in use at line 68 in kbengine/a_bitstr.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/a_bitstr.c | kbengine/a_bitstr.c |
| Line | 117 | 117 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_bitstr.c
Method int i2c_ASN1_BIT_STRING(ASN1_BIT_STRING *a, unsigned char **pp)

```
....
117.      memcpy(p, d, len);
```

Dangerous Functions\Path 5:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=623 |
| Status | New |

The dangerous function, memcpy, was found in use at line 125 in kbengine/a_bitstr.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/a_bitstr.c | kbengine/a_bitstr.c |
| Line | 163 | 163 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_bitstr.c

Method ASN1_BIT_STRING *c2i_ASN1_BIT_STRING(ASN1_BIT_STRING **a,

```
....  
163.         memcpy(s, p, (int)len);
```

Dangerous Functions\Path 6:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=624>

Status New

The dangerous function, memcpy, was found in use at line 245 in kbengine/a_bytes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/a_bytes.c | kbengine/a_bytes.c |
| Line | 283 | 283 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_bytes.c

Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

```
....  
283.         memcpy(&(b.data[num]), os->data, os->length);
```

Dangerous Functions\Path 7:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=625>

Status New

The dangerous function, memcpy, was found in use at line 67 in kbengine/a_bytes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/a_bytes.c | kbengine/a_bytes.c |
| Line | 107 | 107 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_bytes.c

Method ASN1_STRING *d2i_ASN1_type_bytes(ASN1_STRING **a, const unsigned char **pp,

```
....  
107.      memcpy(s, p, (int)len);
```

Dangerous Functions\Path 8:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=626 |
| Status | New |

The dangerous function, memcpy, was found in use at line 129 in kbengine/a_bytes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/a_bytes.c | kbengine/a_bytes.c |
| Line | 151 | 151 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_bytes.c
Method int i2d_ASN1_bytes(ASN1_STRING *a, unsigned char **pp, int tag, int xclass)

```
....  
151.      memcpy(p, a->data, a->length);
```

Dangerous Functions\Path 9:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=627 |
| Status | New |

The dangerous function, memcpy, was found in use at line 157 in kbengine/a_bytes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/a_bytes.c | kbengine/a_bytes.c |
| Line | 212 | 212 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_bytes.c
Method ASN1_STRING *d2i_ASN1_bytes(ASN1_STRING **a, const unsigned char **pp,


```
....  
212.          memcpy(s, p, (int)len);
```

Dangerous Functions\Path 10:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=628 |
| Status | New |

The dangerous function, memcpy, was found in use at line 114 in kbengine/a_int.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/a_int.c | kbengine/a_int.c |
| Line | 160 | 160 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_int.c
Method int i2c_ASN1_INTEGER(ASN1_INTEGER *a, unsigned char **pp)

```
....  
160.          memcpy(p, a->data, (unsigned int)a->length);
```

Dangerous Functions\Path 11:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=629 |
| Status | New |

The dangerous function, memcpy, was found in use at line 186 in kbengine/a_int.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/a_int.c | kbengine/a_int.c |
| Line | 257 | 257 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_int.c
Method ASN1_INTEGER *c2i_ASN1_INTEGER(ASN1_INTEGER **a, const unsigned char **pp,

```
....  
257.          memcpy(s, p, (int)len);
```

Dangerous Functions\Path 12:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=630 |
| Status | New |

The dangerous function, memcpy, was found in use at line 281 in kbengine/a_int.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/a_int.c | kbengine/a_int.c |
| Line | 325 | 325 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_int.c
Method ASN1_INTEGER *d2i_ASN1_INTEGER(ASN1_INTEGER **a, const unsigned char **pp,

```
....  
325.          memcpy(s, p, (int)len);
```

Dangerous Functions\Path 13:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=631 |
| Status | New |

The dangerous function, memcpy, was found in use at line 67 in kbengine/a_object.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/a_object.c | kbengine/a_object.c |
| Line | 81 | 81 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_object.c
Method int i2d_ASN1_OBJECT(ASN1_OBJECT *a, unsigned char **pp)

```
....  
81.      memcpy(p, a->data, a->length);
```

Dangerous Functions\Path 14:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=632 |
| Status | New |

The dangerous function, memcpy, was found in use at line 268 in kbengine/a_object.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/a_object.c | kbengine/a_object.c |
| Line | 322 | 322 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/a_object.c
Method ASN1_OBJECT *c2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....  
322.      memcpy(data, p, length);
```

Dangerous Functions\Path 15:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=633 |
| Status | New |

The dangerous function, memcpy, was found in use at line 447 in kbengine/apr_snprintf.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 471 | 471 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/apr_snprintf.c
Method static char *conv_apr_sockaddr(apr_sockaddr_t *sa, char *buf_end, apr_size_t *len)

```
....
471.          memcpy(p + 1, ipaddr_str, sub_len);
```

Dangerous Functions\Path 16:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=634 |
| Status | New |

The dangerous function, memcpy, was found in use at line 447 in kbengine/apr_snprintf.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 477 | 477 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/apr_snprintf.c
Method static char *conv_apr_sockaddr(apr_sockaddr_t *sa, char *buf_end, apr_size_t *len)

```
....
477.          memcpy(p, ipaddr_str, sub_len);
```

Dangerous Functions\Path 17:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=635 |
| Status | New |

The dangerous function, memcpy, was found in use at line 517 in kbengine/apr_snprintf.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 536 | 536 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/apr_snprintf.c
Method static char *conv_fp(register char format, register double num,

```
.....
536.          memcpy(buf, p, *len + 1);
```

Dangerous Functions\Path 18:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=636 |
| Status | New |

The dangerous function, memcpy, was found in use at line 615 in kbengine/axtls.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/axtls.c | kbengine/axtls.c |
| Line | 633 | 633 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/axtls.c
Method static ssize_t axtls_recv(struct connectdata *conn, /* connection data */

```
.....
633.          memcpy(buf, read_buf,
```

Dangerous Functions\Path 19:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=637 |
| Status | New |

The dangerous function, memcpy, was found in use at line 701 in kbengine/b_print.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/b_print.c | kbengine/b_print.c |
| Line | 720 | 720 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/b_print.c
Method doapr_outh(char **sbuffer,

```
.....  
720.                memcpy(*buffer, *sbuffer, *currlen);
```

Dangerous Functions\Path 20:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=638 |
| Status | New |

The dangerous function, memcpy, was found in use at line 213 in kbengine/cms_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/cms_enc.c | kbengine/cms_enc.c |
| Line | 222 | 222 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/cms_enc.c
Method int cms_EncryptedContent_init(CMS_EncryptedContentInfo *ec,

```
.....  
222.                memcpy(ec->key, key, keylen);
```

Dangerous Functions\Path 21:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=639 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in kbengine/cms_pwri.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/cms_pwri.c | kbengine/cms_pwri.c |
| Line | 265 | 265 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/cms_pwri.c
Method static int kek_unwrap_key(unsigned char *out, size_t *outlen,

```
....  
265.         memcpy(out, tmp + 4, *outlen);
```

Dangerous Functions\Path 22:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=640 |
| Status | New |

The dangerous function, memcpy, was found in use at line 274 in kbengine/cms_pwri.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/cms_pwri.c | kbengine/cms_pwri.c |
| Line | 301 | 301 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/cms_pwri.c
Method static int kek_wrap_key(unsigned char *out, size_t *outlen,

```
....  
301.         memcpy(out + 4, in, inlen);
```

Dangerous Functions\Path 23:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=641 |
| Status | New |

The dangerous function, memcpy, was found in use at line 610 in kbengine/connect.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/connect.c | kbengine/connect.c |
| Line | 612 | 612 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/connect.c
Method void Curl_persistconninfo(struct connectdata *conn)

```
....
612.      memcpy(conn->data->info.conn_primary_ip, conn->primary_ip,
MAX_IPADR_LEN);
```

Dangerous Functions\Path 24:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=642 |
| Status | New |

The dangerous function, memcpy, was found in use at line 610 in kbengine/connect.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/connect.c | kbengine/connect.c |
| Line | 613 | 613 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/connect.c
Method void Curl_persistconninfo(struct connectdata *conn)

```
....
613.      memcpy(conn->data->info.conn_local_ip, conn->local_ip,
MAX_IPADR_LEN);
```

Dangerous Functions\Path 25:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=643 |
| Status | New |

The dangerous function, memcpy, was found in use at line 674 in kbengine/connect.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/connect.c | kbengine/connect.c |
| Line | 709 | 709 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/connect.c
Method void Curl_updateconninfo(struct connectdata *conn, curl_socket_t sockfd)


```
.....  
709.      memcpy(conn->ip_addr_str, conn->primary_ip, MAX_IPADDR_LEN);
```

Dangerous Functions\Path 26:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=644 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1343 in kbengine/connect.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/connect.c | kbengine/connect.c |
| Line | 1370 | 1370 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/connect.c
Method CURLcode Curl_socket(struct connectdata *conn,

```
.....  
1370.      memcpy(&addr->sa_addr, ai->ai_addr, addr->addrlen);
```

Dangerous Functions\Path 27:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=645 |
| Status | New |

The dangerous function, memcpy, was found in use at line 426 in kbengine/cookie.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 725 | 725 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/cookie.c
Method Curl_cookie_add(struct Curl_easy *data,

```
.....  
725.          memcpy(co->path, path, pathlen);
```

Dangerous Functions\Path 28:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=646 |
| Status | New |

The dangerous function, memcpy, was found in use at line 644 in kbengine/crypt_blowfish.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 696 | 696 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/crypt_blowfish.c
Method static char *BF_crypt(const char *key, const char *setting,

```
.....  
696.          memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Dangerous Functions\Path 29:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=647 |
| Status | New |

The dangerous function, memcpy, was found in use at line 644 in kbengine/crypt_blowfish.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 766 | 766 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/crypt_blowfish.c
Method static char *BF_crypt(const char *key, const char *setting,

```
.....  
766.          memcpy(output, setting, 7 + 22 - 1);
```

Dangerous Functions\Path 30:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=648 |
| Status | New |

The dangerous function, memcpy, was found in use at line 814 in kbengine/crypt_blowfish.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 842 | 842 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/crypt_blowfish.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
.....  
842.          memcpy(buf.s, test_setting, sizeof(buf.s));
```

Dangerous Functions\Path 31:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=649 |
| Status | New |

The dangerous function, memcpy, was found in use at line 113 in kbengine/curl_path.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 186 | 186 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_get_pathname(const char **cpp, char **path, char *homedir)

```
....
186.      memcpy(&(*path)[pathLength], cp, (int)(end - cp));
```

Dangerous Functions\Path 32:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=650 |
| Status | New |

The dangerous function, memcpy, was found in use at line 32 in kbengine/curl_path.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 56 | 56 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....
56.      memcpy(real_path, working_path + 3, 4 + working_path_len-3);
```

Dangerous Functions\Path 33:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=651 |
| Status | New |

The dangerous function, memcpy, was found in use at line 32 in kbengine/curl_path.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 58 | 58 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....
58.         memcpy(real_path, working_path, 1 + working_path_len);
```

Dangerous Functions\Path 34:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=652 |
| Status | New |

The dangerous function, memcpy, was found in use at line 32 in kbengine/curl_path.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 70 | 70 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....
70.         memcpy(real_path, homedir, homelen);
```

Dangerous Functions\Path 35:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=653 |
| Status | New |

The dangerous function, memcpy, was found in use at line 32 in kbengine/curl_path.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 74 | 74 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....
74.         memcpy(real_path + homelen + 1, working_path + 3,
```

Dangerous Functions\Path 36:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=654 |
| Status | New |

The dangerous function, memcpy, was found in use at line 32 in kbengine/curl_path.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 84 | 84 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....
84.         memcpy(real_path, working_path, 1 + working_path_len);
```

Dangerous Functions\Path 37:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=655 |
| Status | New |

The dangerous function, memcpy, was found in use at line 580 in kbengine/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 612 | 612 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_both.c
Method static int dtls1_retrieve_buffered_fragment(SSL *s, long max, int *ok)

```
.....  
612.                memcpy(&p[frag->msg_header.frag_off], frag->fragment,
```

Dangerous Functions\Path 38:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=656 |
| Status | New |

The dangerous function, memcpy, was found in use at line 647 in kbengine/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 672 | 672 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr, int *ok)

```
.....  
672.                memcpy(&(frag->msg_header), msg_hdr, sizeof(*msg_hdr));
```

Dangerous Functions\Path 39:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=657 |
| Status | New |

The dangerous function, memcpy, was found in use at line 752 in kbengine/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 809 | 809 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_process_out_of_seq_message(SSL *s, const struct hm_header_st *msg_hdr,

```
.....  
809.          memcpy(&(frag->msg_header), msg_hdr, sizeof(*msg_hdr));
```

Dangerous Functions\Path 40:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=658 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1108 in kbengine/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1124 | 1124 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_both.c
Method int dtls1_buffer_message(SSL *s, int is_ccs)

```
.....  
1124.          memcpy(frag->fragment, s->init_buf->data, s->init_num);
```

Dangerous Functions\Path 41:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=659 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1176 in kbengine/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1213 | 1213 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,


```
....  
1213.      memcpy(s->init_buf->data, frag->fragment,
```

Dangerous Functions\Path 42:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=660 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1176 in kbengine/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1241 | 1241 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

```
....  
1241.      memcpy(save_write_sequence, s->s3->write_sequence,
```

Dangerous Functions\Path 43:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=661 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1176 in kbengine/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1243 | 1243 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

```
.....  
1243.          memcpy(s->s3->write_sequence, s->d1->last_write_sequence,
```

Dangerous Functions\Path 44:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=662 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1176 in kbengine/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1259 | 1259 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

.....
1259. memcpy(s->d1->last_write_sequence, s->s3->write_sequence,

Dangerous Functions\Path 45:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=663 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1176 in kbengine/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1261 | 1261 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

```
.....  
1261.          memcpy(s->s3->write_sequence, save_write_sequence,
```

Dangerous Functions\Path 46:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=664 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1395 in kbengine/d1_both.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1439 | 1439 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_both.c
Method int dtls1_process_heartbeat(SSL *s)

```
.....  
1439.          memcpy(bp, pl, payload);
```

Dangerous Functions\Path 47:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=665 |
| Status | New |

The dangerous function, memcpy, was found in use at line 818 in kbengine/d1_clnt.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_clnt.c | kbengine/d1_clnt.c |
| Line | 859 | 859 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_clnt.c
Method static int dtls1_get_hello_verify(SSL *s)

```
.....  
859.      memcpy(s->d1->cookie, data, cookie_len);
```

Dangerous Functions\Path 48:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=666 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1903 in kbengine/d1_pkt.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 1911 | 1911 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_pkt.c
Method void dtls1_reset_seq_numbers(SSL *s, int rw)

```
.....  
1911.      memcpy(&(s->d1->bitmap), &(s->d1->next_bitmap),  
sizeof(DTLS1_BITMAP));
```

Dangerous Functions\Path 49:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=667 |
| Status | New |

The dangerous function, memcpy, was found in use at line 1903 in kbengine/d1_pkt.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 1915 | 1915 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_pkt.c
Method void dtls1_reset_seq_numbers(SSL *s, int rw)

```
....
1915.          memcpy(s->d1->last_write_sequence, seq,
```

Dangerous Functions\Path 50:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=668 |
| Status | New |

The dangerous function, memcpy, was found in use at line 200 in kbengine/d1_pkt.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 211 | 211 |
| Object | memcpy | memcpy |

Code Snippet

File Name kbengine/d1_pkt.c
Method static int dtls1_copy_record(SSL *s, pitem *item)

```
....
211.          memcpy(&(s->s3->rbuf), &(rdata->rbuf), sizeof(SSL3_BUFFER));
```

Use of Zero Initialized Pointer

Query Path:

CPP\Cx\CPP Medium Threat\Use of Zero Initialized Pointer Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Zero Initialized Pointer\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1300 |
| Status | New |

The variable declared in os at kbengine/a_bytes.c in line 245 is not initialized when it is used by os at kbengine/a_bytes.c in line 245.

| | Source | Destination |
|------|--------------------|--------------------|
| File | kbengine/a_bytes.c | kbengine/a_bytes.c |
| Line | 247 | 283 |

| | | |
|--------|----|----|
| Object | os | os |
|--------|----|----|

Code Snippet

File Name kbengine/a_bytes.c

Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

```

....
247.     ASN1_STRING *os = NULL;
....
283.     memcpy(&(b.data[num]), os->data, os->length);

```

Use of Zero Initialized Pointer\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1301>

Status New

The variable declared in data at kbengine/a_bytes.c in line 245 is not initialized when it is used by data at kbengine/a_bytes.c in line 245.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/a_bytes.c | kbengine/a_bytes.c |
| Line | 253 | 295 |
| Object | data | data |

Code Snippet

File Name kbengine/a_bytes.c

Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

```

....
253.     b.data = NULL;
....
295.     a->data = (unsigned char *)b.data;

```

Use of Zero Initialized Pointer\Path 3:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1302>

Status New

The variable declared in b at kbengine/a_d2i_fp.c in line 86 is not initialized when it is used by data at kbengine/a_d2i_fp.c in line 86.

| | Source | Destination |
|------|---------------------|---------------------|
| File | kbengine/a_d2i_fp.c | kbengine/a_d2i_fp.c |

| | | |
|--------|----|------|
| Line | 88 | 97 |
| Object | b | data |

Code Snippet

File Name kbengine/a_d2i_fp.c

Method void *ASN1_d2i_bio(void *(*xnew) (void), d2i_of_void *d2i, BIO *in, void **x)

```
....
88.     BUF_MEM *b = NULL;
....
97.     p = (unsigned char *)b->data;
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1303>

Status New

The variable declared in b at kbengine/a_d2i_fp.c in line 107 is not initialized when it is used by data at kbengine/a_d2i_fp.c in line 107.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/a_d2i_fp.c | kbengine/a_d2i_fp.c |
| Line | 109 | 118 |
| Object | b | data |

Code Snippet

File Name kbengine/a_d2i_fp.c

Method void *ASN1_item_d2i_bio(const ASN1_ITEM *it, BIO *in, void *x)

```
....
109.    BUF_MEM *b = NULL;
....
118.    p = (const unsigned char *)b->data;
```

Use of Zero Initialized Pointer\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1304>

Status New

The variable declared in ssl at kbengine/axtls.c in line 134 is not initialized when it is used by ssl at kbengine/axtls.c in line 134.

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

| | | |
|--------|------------------|------------------|
| File | kbengine/axtls.c | kbengine/axtls.c |
| Line | 139 | 281 |
| Object | ssl | ssl |

Code Snippet

File Name kbengine/axtls.c

Method static CURLcode connect_prep(struct connectdata *conn, int sockindex)

```
....
139.     SSL *ssl = NULL;
....
281.     BACKEND->ssl = ssl;
```

Use of Zero Initialized Pointer\Path 6:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1305>

Status New

The variable declared in tkey at kbengine/cms_enc.c in line 70 is not initialized when it is used by key at kbengine/cms_enc.c in line 70.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/cms_enc.c | kbengine/cms_enc.c |
| Line | 146 | 169 |
| Object | tkey | key |

Code Snippet

File Name kbengine/cms_enc.c

Method BIO *cms_EncryptedContent_init_bio(CMS_EncryptedContentInfo *ec)

```
....
146.         tkey = NULL;
....
169.         ec->key = tkey;
```

Use of Zero Initialized Pointer\Path 7:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1306>

Status New

The variable declared in tkey at kbengine/cms_enc.c in line 70 is not initialized when it is used by key at kbengine/cms_enc.c in line 70.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/cms_enc.c | kbengine/cms_enc.c |
| Line | 77 | 169 |
| Object | tkey | key |

Code Snippet

File Name kbengine/cms_enc.c
Method BIO *cms_EncryptedContent_init_bio(CMS_EncryptedContentInfo *ec)

```
....
77.         unsigned char *tkey = NULL;
....
169.         ec->key = tkey;
```

Use of Zero Initialized Pointer\Path 8:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1307>
Status New

The variable declared in tok_buf at kbengine/cookie.c in line 426 is not initialized when it is used by lastc at kbengine/cookie.c in line 426.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 749 | 983 |
| Object | tok_buf | lastc |

Code Snippet

File Name kbengine/cookie.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
749.         char *tok_buf = NULL;
....
983.         lastc = clist;
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1308>
Status New

The variable declared in tok_buf at kbengine/cookie.c in line 426 is not initialized when it is used by lastc at kbengine/cookie.c in line 426.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 749 | 977 |
| Object | tok_buf | lastc |

Code Snippet

File Name kbengine/cookie.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
749.      char *tok_buf = NULL;
....
977.      lastc = clist;
```

Use of Zero Initialized Pointer\Path 10:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1309 |
| Status | New |

The variable declared in tok_buf at kbengine/cookie.c in line 426 is not initialized when it is used by cookies at kbengine/cookie.c in line 377.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 749 | 385 |
| Object | tok_buf | cookies |

Code Snippet

File Name kbengine/cookie.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
749.      char *tok_buf = NULL;
```

File Name kbengine/cookie.c
Method static void remove_expired(struct CookieInfo *cookies)

```
....
385.      co = cookies->cookies[i];
```

Use of Zero Initialized Pointer\Path 11:

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

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1310](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1310)

Status New

The variable declared in tok_buf at kbengine/cookie.c in line 426 is not initialized when it is used by cookies at kbengine/cookie.c in line 426.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 749 | 910 |
| Object | tok_buf | cookies |

Code Snippet

File Name kbengine/cookie.c

Method Curl_cookie_add(struct Curl_easy *data,

```
....  
749.      char *tok_buf = NULL;  
....  
910.      clist = c->cookies[myhash];
```

Use of Zero Initialized Pointer\Path 12:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1311>

Status New

The variable declared in tok_buf at kbengine/cookie.c in line 426 is not initialized when it is used by cookies at kbengine/cookie.c in line 426.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 749 | 999 |
| Object | tok_buf | cookies |

Code Snippet

File Name kbengine/cookie.c

Method Curl_cookie_add(struct Curl_easy *data,

```
....  
749.      char *tok_buf = NULL;  
....  
999.      c->cookies[myhash] = co;
```

Use of Zero Initialized Pointer\Path 13:

Severity Medium

Result State To Verify

Online Results <http://WIN->

| | |
|--------|--|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1312 |
| Status | New |

The variable declared in tok_buf at kbengine/cookie.c in line 426 is not initialized when it is used by first at kbengine/cookie.c in line 242.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 749 | 253 |
| Object | tok_buf | first |

Code Snippet

File Name kbengine/cookie.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
749.      char *tok_buf = NULL;
```

File Name kbengine/cookie.c
Method static const char *get_top_domain(const char * const domain, size_t *outlen)

```
....
253.      first = memchr(domain, '.', (last - domain));
```

Use of Zero Initialized Pointer\Path 14:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1313 |
| Status | New |

The variable declared in mainco at kbengine/cookie.c in line 1215 is not initialized when it is used by mainco at kbengine/cookie.c in line 1215.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1222 | 1265 |
| Object | mainco | mainco |

Code Snippet

File Name kbengine/cookie.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```

.....
1222.      struct Cookie *mainco = NULL;
.....
1265.              mainco = newco;

```

Use of Zero Initialized Pointer\Path 15:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1314 |
| Status | New |

The variable declared in mainco at kbengine/cookie.c in line 1215 is not initialized when it is used by mainco at kbengine/cookie.c in line 1215.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1222 | 1303 |
| Object | mainco | mainco |

Code Snippet

File Name kbengine/cookie.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```

.....
1222.      struct Cookie *mainco = NULL;
.....
1303.              mainco = array[0]; /* start here */

```

Use of Zero Initialized Pointer\Path 16:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1315 |
| Status | New |

The variable declared in list at kbengine/cookie.c in line 1529 is not initialized when it is used by list at kbengine/cookie.c in line 1529.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1531 | 1556 |
| Object | list | list |

Code Snippet

File Name kbengine/cookie.c
Method static struct curl_slist *cookie_list(struct Curl_easy *data)

```

....
1531.      struct curl_slist *list = NULL;
....
1556.          list = beg;

```

Use of Zero Initialized Pointer\Path 17:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1316 |
| Status | New |

The variable declared in buf at kbengine/d1_both.c in line 174 is not initialized when it is used by frag at kbengine/d1_both.c in line 174.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 178 | 194 |
| Object | buf | frag |

Code Snippet

File Name kbengine/d1_both.c
Method static hm_fragment *dtls1_hm_fragment_new(unsigned long frag_len,

```

....
178.      unsigned char *buf = NULL;
....
194.      frag->fragment = buf;

```

Use of Zero Initialized Pointer\Path 18:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1317 |
| Status | New |

The variable declared in frag at kbengine/d1_both.c in line 647 is not initialized when it is used by reassembly at kbengine/d1_both.c in line 647.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 679 | 714 |
| Object | frag | reassembly |

Code Snippet

File Name kbengine/d1_both.c

Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr, int *ok)

```
....
679.             frag = NULL;
....
714.             RSMBLY_BITMASK_MARK(frag->reassemble, (long)msg_hdr->frag_off,
```

Use of Zero Initialized Pointer\Path 19:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1318 |
| Status | New |

The variable declared in reassembly at kbengine/d1_both.c in line 647 is not initialized when it is used by frag at kbengine/d1_both.c in line 647.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 722 | 721 |
| Object | reassemble | frag |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr, int *ok)

```
....
722.             frag->reassemble = NULL;
....
721.             OPENSSL_free(frag->reassemble);
```

Use of Zero Initialized Pointer\Path 20:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1319 |
| Status | New |

The variable declared in frag at kbengine/d1_both.c in line 647 is not initialized when it is used by frag at kbengine/d1_both.c in line 647.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 679 | 721 |
| Object | frag | frag |

Code Snippet

File Name kbengine/d1_both.c

Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr, int *ok)

```
....
679.             frag = NULL;
....
721.             OPENSSL_free(frag->reassembly);
```

Use of Zero Initialized Pointer\Path 21:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1320>

Status New

The variable declared in frag at kbengine/d1_both.c in line 647 is not initialized when it is used by reassembly at kbengine/d1_both.c in line 647.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 679 | 714 |
| Object | frag | reassembly |

Code Snippet

File Name kbengine/d1_both.c

Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr, int *ok)

```
....
679.             frag = NULL;
....
714.             RSMBLY_BITMASK_MARK(frag->reassembly, (long)msg_hdr->frag_off,
```

Use of Zero Initialized Pointer\Path 22:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1321>

Status New

The variable declared in frag at kbengine/d1_both.c in line 647 is not initialized when it is used by reassembly at kbengine/d1_both.c in line 647.

| | Source | Destination |
|------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 679 | 714 |

| | | |
|--------|------|------------|
| Object | frag | reassembly |
|--------|------|------------|

Code Snippet

File Name kbengine/d1_both.c

Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr, int *ok)

```
....
679.             frag = NULL;
....
714.             RSMBLY_BITMASK_MARK(frag->reassembly, (long)msg_hdr->frag_off,
```

Use of Zero Initialized Pointer\Path 23:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1322>

Status New

The variable declared in frag at kbengine/d1_both.c in line 647 is not initialized when it is used by frag at kbengine/d1_both.c in line 647.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 679 | 707 |
| Object | frag | frag |

Code Snippet

File Name kbengine/d1_both.c

Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr, int *ok)

```
....
679.             frag = NULL;
....
707.             frag->fragment + msg_hdr-
>frag_off,
```

Use of Zero Initialized Pointer\Path 24:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1323>

Status New

The variable declared in bitmask at kbengine/d1_both.c in line 174 is not initialized when it is used by reassembly at kbengine/d1_both.c in line 174.

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

| | | |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 179 | 209 |
| Object | bitmask | reassembly |

Code Snippet

File Name kbengine/d1_both.c

Method static hm_fragment *dtls1_hm_fragment_new(unsigned long frag_len,

```
....
179.         unsigned char *bitmask = NULL;
....
209.         frag->reassembly = bitmask;
```

Use of Zero Initialized Pointer\Path 25:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1324>

Status New

The variable declared in dest_len at kbengine/d1_pkt.c in line 771 is not initialized when it is used by dest_len at kbengine/d1_pkt.c in line 771.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 981 | 1050 |
| Object | dest_len | dest_len |

Code Snippet

File Name kbengine/d1_pkt.c

Method int dtls1_read_bytes(SSL *s, int type, unsigned char *buf, int len, int peek)

```
....
981.         unsigned int *dest_len = NULL;
....
1050.         *dest_len = dest_maxlen;
```

Use of Zero Initialized Pointer\Path 26:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1325>

Status New

The variable declared in database at kbengine/dict.c in line 126 is not initialized when it is used by database at kbengine/dict.c in line 126.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/dict.c | kbengine/dict.c |
| Line | 131 | 192 |
| Object | database | database |

Code Snippet

File Name kbengine/dict.c

Method static CURLcode dict_do(struct connectdata *conn, bool *done)

```
....
131.     char *database = NULL;
....
192.                                     database,
```

Use of Zero Initialized Pointer\Path 27:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1326>

Status New

The variable declared in strategy at kbengine/dict.c in line 126 is not initialized when it is used by strategy at kbengine/dict.c in line 126.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/dict.c | kbengine/dict.c |
| Line | 132 | 193 |
| Object | strategy | strategy |

Code Snippet

File Name kbengine/dict.c

Method static CURLcode dict_do(struct connectdata *conn, bool *done)

```
....
132.     char *strategy = NULL;
....
193.                                     strategy,
```

Use of Zero Initialized Pointer\Path 28:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1327>

Status New

The variable declared in rwlock at kbengine/filestat.c in line 217 is not initialized when it is used by rwlock at kbengine/filestat.c in line 217.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/filestat.c | kbengine/filestat.c |
| Line | 221 | 247 |
| Object | rwlock | rwlock |

Code Snippet

File Name kbengine/filestat.c

Method int cstat (NXPathCtx_t ctx, char *path, struct stat *buf, unsigned long requestmap, apr_pool_t *p)

```
....
221.      apr_thread_rwlock_t *rwlock = NULL;
....
247.      apr_pool_userdata_set ((void*)rwlock,
"STAT_CACHE_LOCK", apr_pool_cleanup_null, gPool);
```

Use of Zero Initialized Pointer\Path 29:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1328>

Status New

The variable declared in path at kbengine/ftp.c in line 3143 is not initialized when it is used by prevpath at kbengine/ftp.c in line 3210.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 3143 | 3210 |
| Object | path | prevpath |

Code Snippet

File Name kbengine/ftp.c

Method static CURLcode ftp_done(struct connectdata *conn, CURLcode status,

```
....
3143.      char *path = NULL;
....
3210.      ftpc->prevpath = path;
```

Use of Zero Initialized Pointer\Path 30:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1329>

Status New

The variable declared in ludp at kbengine/ldap.c in line 253 is not initialized when it is used by ludp at kbengine/ldap.c in line 253.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/ldap.c | kbengine/ldap.c |
| Line | 258 | 482 |
| Object | ludp | ludp |

Code Snippet

File Name kbengine/ldap.c
Method

```
....  
258.     LDAP *server = NULL;  
....  
482.     rc = ldap_search_s(server, ludp->lud_dn, ludp->lud_scope,
```

Use of Zero Initialized Pointer\Path 31:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1330 |
| Status | New |

The variable declared in ludp at kbengine/ldap.c in line 253 is not initialized when it is used by ludp at kbengine/ldap.c in line 253.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/ldap.c | kbengine/ldap.c |
| Line | 258 | 482 |
| Object | ludp | ludp |

Code Snippet

File Name kbengine/ldap.c
Method

```
....  
258.     LDAP *server = NULL;  
....  
482.     rc = ldap_search_s(server, ludp->lud_dn, ludp->lud_scope,
```

Use of Zero Initialized Pointer\Path 32:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1331 |
| Status | New |

The variable declared in ludp at kbengine/ldap.c in line 253 is not initialized when it is used by ludp at kbengine/ldap.c in line 253.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/ldap.c | kbengine/ldap.c |
| Line | 258 | 481 |
| Object | ludp | ludp |

Code Snippet

File Name kbengine/ldap.c
Method

```
....  
258.     LDAP *server = NULL;  
....  
481.
```

Use of Zero Initialized Pointer\Path 33:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1332 |
| Status | New |

The variable declared in ludp at kbengine/ldap.c in line 253 is not initialized when it is used by ludp at kbengine/ldap.c in line 253.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/ldap.c | kbengine/ldap.c |
| Line | 258 | 481 |
| Object | ludp | ludp |

Code Snippet

File Name kbengine/ldap.c
Method

```
....  
258.     LDAP *server = NULL;  
....  
481.
```

Use of Zero Initialized Pointer\Path 34:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1333 |
| Status | New |

The variable declared in user at kbengine/ldap.c in line 253 is not initialized when it is used by inuser at kbengine/ldap.c in line 226.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/ldap.c | kbengine/ldap.c |
| Line | 276 | 235 |
| Object | user | inuser |

Code Snippet

File Name kbengine/ldap.c
Method

```
....  
276. #endif
```

File Name kbengine/ldap.c
Method

```
....  
235. if(user && passwd && (conn->data->set.httppauth &  
CURLAUTH_BASIC)) {
```

Use of Zero Initialized Pointer\Path 35:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1334 |
| Status | New |

The variable declared in passwd at kbengine/ldap.c in line 253 is not initialized when it is used by inpass at kbengine/ldap.c in line 226.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/ldap.c | kbengine/ldap.c |
| Line | 277 | 236 |
| Object | passwd | inpass |

Code Snippet

File Name kbengine/ldap.c
Method

```
....  
277. char *user = NULL;
```

File Name kbengine/ldap.c

Method

```
....  
236.      inuser = Curl_convert_UTF8_to_tchar((char *) user);
```

Use of Zero Initialized Pointer\Path 36:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1335 |
| Status | New |

The variable declared in ufds at kbengine/multi.c in line 988 is not initialized when it is used by ufds at kbengine/multi.c in line 988.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 1000 | 1120 |
| Object | ufds | ufds |

Code Snippet

File Name kbengine/multi.c
Method CURLMcode curl_multi_wait(struct Curl_multi *multi,

```
....  
1000.      struct pollfd *ufds = NULL;  
....  
1120.      unsigned r = ufds[curlfds + i].revents;
```

Use of Zero Initialized Pointer\Path 37:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1336 |
| Status | New |

The variable declared in newurl at kbengine/multi.c in line 1327 is not initialized when it is used by msg at kbengine/multi.c in line 1327.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 1882 | 2139 |
| Object | newurl | msg |

Code Snippet

File Name kbengine/multi.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,


```
.....
1882.      char *newurl = NULL;
.....
2139.      msg->extmsg.data.result = result;
```

Use of Zero Initialized Pointer\Path 38:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1337 |
| Status | New |

The variable declared in Pointer at kbengine/multi.c in line 515 is not initialized when it is used by msg at kbengine/multi.c in line 1327.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 654 | 2139 |
| Object | Pointer | msg |

Code Snippet

File Name kbengine/multi.c
Method static CURLcode multi_done(struct connectdata **connp,

```
.....
654.      *connp = NULL; /* to make the caller of this function better
detect that
```

File Name kbengine/multi.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
.....
2139.      msg->extmsg.data.result = result;
```

Use of Zero Initialized Pointer\Path 39:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1338 |
| Status | New |

The variable declared in easy_conn at kbengine/multi.c in line 1327 is not initialized when it is used by msg at kbengine/multi.c in line 1327.

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

| | | |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 1532 | 2139 |
| Object | easy_conn | msg |

Code Snippet

File Name kbengine/multi.c

Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
1532.         data->easy_conn = NULL;           /* no more connection
*/
....
2139.         msg->extmsg.data.result = result;
```

Use of Zero Initialized Pointer\Path 40:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1339>

Status New

The variable declared in newurl at kbengine/multi.c in line 1327 is not initialized when it is used by msg at kbengine/multi.c in line 1327.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 1707 | 2139 |
| Object | newurl | msg |

Code Snippet

File Name kbengine/multi.c

Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
1707.         char *newurl = NULL;
....
2139.         msg->extmsg.data.result = result;
```

Use of Zero Initialized Pointer\Path 41:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1340>

Status New

The variable declared in easy_conn at kbengine/multi.c in line 1327 is not initialized when it is used by msg at kbengine/multi.c in line 1327.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 2050 | 2139 |
| Object | easy_conn | msg |

Code Snippet

File Name kbengine/multi.c

Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....  
2050.          data->easy_conn = NULL;  
....  
2139.          msg->extmsg.data.result = result;
```

Use of Zero Initialized Pointer\Path 42:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1341>

Status New

The variable declared in easy_conn at kbengine/multi.c in line 1327 is not initialized when it is used by msg at kbengine/multi.c in line 1327.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 2108 | 2139 |
| Object | easy_conn | msg |

Code Snippet

File Name kbengine/multi.c

Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....  
2108.          data->easy_conn = NULL;  
....  
2139.          msg->extmsg.data.result = result;
```

Use of Zero Initialized Pointer\Path 43:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1342>

Status New

The variable declared in dns_entry at kbengine/multi.c in line 515 is not initialized when it is used by msg at kbengine/multi.c in line 1327.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 592 | 2139 |
| Object | dns_entry | msg |

Code Snippet

File Name kbengine/multi.c

Method static CURLcode multi_done(struct connectdata **connp,

```
....
592.     conn->dns_entry = NULL;
```



File Name kbengine/multi.c

Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2139.     msg->extmsg.data.result = result;
```

Use of Zero Initialized Pointer\Path 44:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1343>

Status New

The variable declared in location at kbengine/multi.c in line 515 is not initialized when it is used by msg at kbengine/multi.c in line 1327.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 547 | 2139 |
| Object | location | msg |

Code Snippet

File Name kbengine/multi.c

Method static CURLcode multi_done(struct connectdata **connp,

```
....
547.     data->req.location = NULL;
```



File Name kbengine/multi.c

Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2139.          msg->extmsg.data.result = result;
```

Use of Zero Initialized Pointer\Path 45:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1344 |
| Status | New |

The variable declared in newurl at kbengine/multi.c in line 515 is not initialized when it is used by msg at kbengine/multi.c in line 1327.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 545 | 2139 |
| Object | newurl | msg |

Code Snippet

File Name kbengine/multi.c
Method static CURLcode multi_done(struct connectdata **connp,

```
....
545.      data->req.newurl = NULL;
```

File Name kbengine/multi.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2139.          msg->extmsg.data.result = result;
```

Use of Zero Initialized Pointer\Path 46:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1345 |
| Status | New |

The variable declared in Pointer at kbengine/multi.c in line 1194 is not initialized when it is used by msg at kbengine/multi.c in line 1327.

| | Source | Destination |
|------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 1213 | 2139 |

| | | |
|--------|---------|-----|
| Object | Pointer | msg |
|--------|---------|-----|

Code Snippet

File Name kbengine/multi.c

Method static CURLcode multi_reconnect_request(struct connectdata **connp)

```
....
1213.     *connp = NULL;
```



File Name kbengine/multi.c

Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2139.         msg->extmsg.data.result = result;
```

Use of Zero Initialized Pointer\Path 47:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1346>

Status New

The variable declared in os at kbengine/rsa_ameth.c in line 531 is not initialized when it is used by os at kbengine/rsa_ameth.c in line 708.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/rsa_ameth.c | kbengine/rsa_ameth.c |
| Line | 535 | 726 |
| Object | os | os |

Code Snippet

File Name kbengine/rsa_ameth.c

Method static ASN1_STRING *rsa_ctx_to_pss(EVP_PKEY_CTX *pkctx)

```
....
535.     ASN1_STRING *os = NULL;
```



File Name kbengine/rsa_ameth.c

Method static int rsa_cms_sign(CMS_SignerInfo *si)

```
....
726.         os = rsa_ctx_to_pss(pkctx);
```

Use of Zero Initialized Pointer\Path 48:

Severity Medium

| | |
|----------------|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1347 |
| Status | New |

The variable declared in os at kbengine/rsa_ameth.c in line 531 is not initialized when it is used by os1 at kbengine/rsa_ameth.c in line 733.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/rsa_ameth.c | kbengine/rsa_ameth.c |
| Line | 535 | 745 |
| Object | os | os1 |

Code Snippet

File Name kbengine/rsa_ameth.c
Method static ASN1_STRING *rsa_ctx_to_pss(EVP_PKEY_CTX *pkctx)

```
....
535.     ASN1_STRING *os = NULL;
```



File Name kbengine/rsa_ameth.c
Method static int rsa_item_sign(EVP_MD_CTX *ctx, const ASN1_ITEM *it, void *asn,

```
....
745.     os1 = rsa_ctx_to_pss(pkctx);
```

Use of Zero Initialized Pointer\Path 49:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1348 |
| Status | New |

The variable declared in pref_cipher at kbengine/s3_clnt.c in line 893 is not initialized when it is used by sk at kbengine/s3_clnt.c in line 893.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_clnt.c | kbengine/s3_clnt.c |
| Line | 1002 | 1070 |
| Object | pref_cipher | sk |

Code Snippet

File Name kbengine/s3_clnt.c
Method int ssl3_get_server_hello(SSL *s)

```
.....
1002.          SSL_CIPHER *pref_cipher = NULL;
.....
1070.          sk = ssl_get_ciphers_by_id(s);
```

Use of Zero Initialized Pointer\Path 50:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1349 |
| Status | New |

The variable declared in peer at kbengine/s3_clnt.c in line 1172 is not initialized when it is used by sk at kbengine/s3_clnt.c in line 893.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_clnt.c | kbengine/s3_clnt.c |
| Line | 1345 | 1070 |
| Object | peer | sk |

Code Snippet

File Name kbengine/s3_clnt.c
Method int ssl3_get_server_certificate(SSL *s)

```
.....
1345.          s->session->peer = NULL;
```

File Name kbengine/s3_clnt.c
Method int ssl3_get_server_hello(SSL *s)

```
.....
1070.          sk = ssl_get_ciphers_by_id(s);
```

Buffer Overflow boundcpy WrongSizeParam

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundcpy WrongSizeParam Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow boundcpy WrongSizeParam\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1349 |

[33&pathid=195](#)

Status New

The size of the buffer used by *BF_crypt in Namespace1873623869, at line 644 of kbengine/crypt_blowfish.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *BF_crypt passes to Namespace1873623869, at line 644 of kbengine/crypt_blowfish.c, to overwrite the target buffer.

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 696 | 696 |
| Object | Namespace1873623869 | Namespace1873623869 |

Code Snippet

File Name kbengine/crypt_blowfish.c

Method static char *BF_crypt(const char *key, const char *setting,

```
....  
696.      memcpy(data.ctx.S, BF_init_state.S, sizeof(data.ctx.S));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=196>

Status New

The size of the buffer used by *_crypt_blowfish_rn in Namespace1873623869, at line 814 of kbengine/crypt_blowfish.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *_crypt_blowfish_rn passes to Namespace1873623869, at line 814 of kbengine/crypt_blowfish.c, to overwrite the target buffer.

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 842 | 842 |
| Object | Namespace1873623869 | Namespace1873623869 |

Code Snippet

File Name kbengine/crypt_blowfish.c

Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....  
842.      memcpy(buf.s, test_setting, sizeof(buf.s));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=197>

Status New

The size of the buffer used by `dtls1_reassemble_fragment` in `msg_hdr`, at line 647 of `kbengine/d1_both.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `dtls1_reassemble_fragment` passes to `msg_hdr`, at line 647 of `kbengine/d1_both.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 672 | 672 |
| Object | msg_hdr | msg_hdr |

Code Snippet

File Name kbengine/d1_both.c

Method `dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr, int *ok)`

```
....  
672.          memcpy(&(frag->msg_header), msg_hdr, sizeof(*msg_hdr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=198>

Status New

The size of the buffer used by `dtls1_process_out_of_seq_message` in `msg_hdr`, at line 752 of `kbengine/d1_both.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `dtls1_process_out_of_seq_message` passes to `msg_hdr`, at line 752 of `kbengine/d1_both.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 809 | 809 |
| Object | msg_hdr | msg_hdr |

Code Snippet

File Name kbengine/d1_both.c

Method `dtls1_process_out_of_seq_message(SSL *s, const struct hm_header_st *msg_hdr,`

```
....  
809.          memcpy(&(frag->msg_header), msg_hdr, sizeof(*msg_hdr));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=198>

[33&pathid=199](#)

Status New

The size of the buffer used by dtls1_retransmit_message in ->, at line 1176 of kbengine/d1_both.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_retransmit_message passes to ->, at line 1176 of kbengine/d1_both.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1242 | 1242 |
| Object | -> | -> |

Code Snippet

File Name kbengine/d1_both.c

Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

```
.....  
1242.                sizeof(s->s3->write_sequence));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=200>

Status New

The size of the buffer used by dtls1_retransmit_message in ->, at line 1176 of kbengine/d1_both.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_retransmit_message passes to ->, at line 1176 of kbengine/d1_both.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1244 | 1244 |
| Object | -> | -> |

Code Snippet

File Name kbengine/d1_both.c

Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

```
.....  
1244.                sizeof(s->s3->write_sequence));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=201>

Status New

The size of the buffer used by dtls1_retransmit_message in ->, at line 1176 of kbengine/d1_both.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_retransmit_message passes to ->, at line 1176 of kbengine/d1_both.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1260 | 1260 |
| Object | -> | -> |

Code Snippet

File Name kbengine/d1_both.c

Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

```
.....  
1260.                sizeof(s->s3->write_sequence));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=202>

Status New

The size of the buffer used by dtls1_retransmit_message in ->, at line 1176 of kbengine/d1_both.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_retransmit_message passes to ->, at line 1176 of kbengine/d1_both.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1262 | 1262 |
| Object | -> | -> |

Code Snippet

File Name kbengine/d1_both.c

Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

```
.....  
1262.                sizeof(s->s3->write_sequence));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=203>

Status New

The size of the buffer used by `dtls1_reset_seq_numbers` in `DTLS1_BITMAP`, at line 1903 of `kbengine/d1_pkt.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `dtls1_reset_seq_numbers` passes to `DTLS1_BITMAP`, at line 1903 of `kbengine/d1_pkt.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 1911 | 1911 |
| Object | DTLS1_BITMAP | DTLS1_BITMAP |

Code Snippet

File Name kbengine/d1_pkt.c

Method void dtls1_reset_seq_numbers(SSL *s, int rw)

```
....  
1911.          memcpy(&(s->d1->bitmap), &(s->d1->next_bitmap),  
sizeof(DTLS1_BITMAP));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=204>

Status New

The size of the buffer used by `dtls1_reset_seq_numbers` in `->`, at line 1903 of `kbengine/d1_pkt.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `dtls1_reset_seq_numbers` passes to `->`, at line 1903 of `kbengine/d1_pkt.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 1916 | 1916 |
| Object | -> | -> |

Code Snippet

File Name kbengine/d1_pkt.c

Method void dtls1_reset_seq_numbers(SSL *s, int rw)

```
....  
1916.          sizeof(s->s3->write_sequence));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=205>

Status New

The size of the buffer used by dtls1_copy_record in SSL3_BUFFER, at line 200 of kbengine/d1_pkt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_copy_record passes to SSL3_BUFFER, at line 200 of kbengine/d1_pkt.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 211 | 211 |
| Object | SSL3_BUFFER | SSL3_BUFFER |

Code Snippet

File Name kbengine/d1_pkt.c

Method static int dtls1_copy_record(SSL *s, pitem *item)

```
....  
211.      memcpy(&(s->s3->rbuf), &(rdata->rbuf), sizeof(SSL3_BUFFER));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=206>

Status New

The size of the buffer used by dtls1_copy_record in SSL3_RECORD, at line 200 of kbengine/d1_pkt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_copy_record passes to SSL3_RECORD, at line 200 of kbengine/d1_pkt.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 212 | 212 |
| Object | SSL3_RECORD | SSL3_RECORD |

Code Snippet

File Name kbengine/d1_pkt.c

Method static int dtls1_copy_record(SSL *s, pitem *item)

```
....  
212.      memcpy(&(s->s3->rrec), &(rdata->rrec), sizeof(SSL3_RECORD));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=207>

Status New

The size of the buffer used by `dtls1_buffer_record` in `SSL3_BUFFER`, at line 221 of `kbengine/d1_pkt.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `dtls1_buffer_record` passes to `SSL3_BUFFER`, at line 221 of `kbengine/d1_pkt.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 244 | 244 |
| Object | SSL3_BUFFER | SSL3_BUFFER |

Code Snippet

File Name kbengine/d1_pkt.c

Method `dtls1_buffer_record(SSL *s, record_pqueue *queue, unsigned char *priority)`

```
....  
244.      memcpy(&(rdata->rbuf), &(s->s3->rbuf), sizeof(SSL3_BUFFER));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=208>

Status New

The size of the buffer used by `dtls1_buffer_record` in `SSL3_RECORD`, at line 221 of `kbengine/d1_pkt.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `dtls1_buffer_record` passes to `SSL3_RECORD`, at line 221 of `kbengine/d1_pkt.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 245 | 245 |
| Object | SSL3_RECORD | SSL3_RECORD |

Code Snippet

File Name kbengine/d1_pkt.c

Method `dtls1_buffer_record(SSL *s, record_pqueue *queue, unsigned char *priority)`

```
....  
245.      memcpy(&(rdata->rrec), &(s->s3->rrec), sizeof(SSL3_RECORD));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=209>

Status New

The size of the buffer used by `dtls1_accept` in `->`, at line 162 of `kbengine/d1_srvr.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `dtls1_accept` passes to `->`, at line 162 of `kbengine/d1_srvr.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_srvr.c | kbengine/d1_srvr.c |
| Line | 355 | 355 |
| Object | -> | -> |

Code Snippet

File Name kbengine/d1_srvr.c
Method `int dtls1_accept(SSL *s)`

```
....  
355.                                sizeof(s->s3->write_sequence));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=210 |
| Status | New |

The size of the buffer used by `multi_addtimeout` in `stamp`, at line 2905 of `kbengine/multi.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `multi_addtimeout` passes to `stamp`, at line 2905 of `kbengine/multi.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 2918 | 2918 |
| Object | stamp | stamp |

Code Snippet

File Name kbengine/multi.c
Method `multi_addtimeout(struct Curl_easy *data,`

```
....  
2918.     memcpy(&node->time, stamp, sizeof(*stamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=211 |
| Status | New |

The size of the buffer used by `bindlocal` in `Curl_sockaddr_storage`, at line 241 of `kbengine/connect.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source

buffer that bindlocal passes to Curl_sockaddr_storage, at line 241 of kbengine/connect.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-----------------------|-----------------------|
| File | kbengine/connect.c | kbengine/connect.c |
| Line | 269 | 269 |
| Object | Curl_sockaddr_storage | Curl_sockaddr_storage |

Code Snippet

File Name kbengine/connect.c

Method static CURLcode bindlocal(struct connectdata *conn,

```
....  
269.      memset(&sa, 0, sizeof(struct Curl_sockaddr_storage));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=212>

Status New

The size of the buffer used by bindlocal in Curl_sockaddr_storage, at line 241 of kbengine/connect.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bindlocal passes to Curl_sockaddr_storage, at line 241 of kbengine/connect.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-----------------------|-----------------------|
| File | kbengine/connect.c | kbengine/connect.c |
| Line | 447 | 447 |
| Object | Curl_sockaddr_storage | Curl_sockaddr_storage |

Code Snippet

File Name kbengine/connect.c

Method static CURLcode bindlocal(struct connectdata *conn,

```
....  
447.      memset(&add, 0, sizeof(struct Curl_sockaddr_storage));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=213>

Status New

The size of the buffer used by *_crypt_blowfish_rn in Namespace1873623869, at line 814 of kbengine/crypt_blowfish.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that *_crypt_blowfish_rn passes to Namespace1873623869, at line 814 of kbengine/crypt_blowfish.c, to overwrite the target buffer.

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 845 | 845 |
| Object | Namespace1873623869 | Namespace1873623869 |

Code Snippet

File Name kbengine/crypt_blowfish.c

Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
....  
845.      memset(buf.o, 0x55, sizeof(buf.o));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=214>

Status New

The size of the buffer used by dtls1_get_message in hm_header_st, at line 456 of kbengine/d1_both.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_get_message passes to hm_header_st, at line 456 of kbengine/d1_both.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 481 | 481 |
| Object | hm_header_st | hm_header_st |

Code Snippet

File Name kbengine/d1_both.c

Method long dtls1_get_message(SSL *s, int st1, int stn, int mt, long max, int *ok)

```
....  
481.      memset(msg_hdr, 0x00, sizeof(struct hm_header_st));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=215>

Status New

The size of the buffer used by dtls1_get_message in hm_header_st, at line 456 of kbengine/d1_both.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source

buffer that `dtls1_get_message` passes to `hm_header_st`, at line 456 of `kbengine/d1_both.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 517 | 517 |
| Object | hm_header_st | hm_header_st |

Code Snippet

File Name kbengine/d1_both.c

Method `long dtls1_get_message(SSL *s, int st1, int stn, int mt, long max, int *ok)`

```
....  
517.      memset(msg_hdr, 0x00, sizeof(struct hm_header_st));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=216>

Status New

The size of the buffer used by `dtls1_get_message_header` in `hm_header_st`, at line 1351 of `kbengine/d1_both.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `dtls1_get_message_header` passes to `hm_header_st`, at line 1351 of `kbengine/d1_both.c`, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1353 | 1353 |
| Object | hm_header_st | hm_header_st |

Code Snippet

File Name kbengine/d1_both.c

Method `dtls1_get_message_header(unsigned char *data, struct hm_header_st *msg_hdr)`

```
....  
1353.      memset(msg_hdr, 0x00, sizeof(struct hm_header_st));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=217>

Status New

The size of the buffer used by `dtls1_get_ccs_header` in `ccs_header_st`, at line 1362 of `kbengine/d1_both.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that dtls1_get_ccs_header passes to ccs_header_st, at line 1362 of kbengine/d1_both.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1364 | 1364 |
| Object | ccs_header_st | ccs_header_st |

Code Snippet

File Name kbengine/d1_both.c

Method void dtls1_get_ccs_header(unsigned char *data, struct ccs_header_st *ccs_hdr)

```
....  
1364.      memset(ccs_hdr, 0x00, sizeof(struct ccs_header_st));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=218>

Status New

The size of the buffer used by dtls1_connect in ->, at line 164 of kbengine/d1_clnt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_connect passes to ->, at line 164 of kbengine/d1_clnt.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_clnt.c | kbengine/d1_clnt.c |
| Line | 274 | 274 |
| Object | -> | -> |

Code Snippet

File Name kbengine/d1_clnt.c

Method int dtls1_connect(SSL *s)

```
....  
274.      memset(s->s3->client_random, 0, sizeof(s->s3->client_random));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=219>

Status New

The size of the buffer used by dtls1_reset_seq_numbers in DTLS1_BITMAP, at line 1903 of kbengine/d1_pkt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that dtls1_reset_seq_numbers passes to DTLS1_BITMAP, at line 1903 of kbengine/d1_pkt.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 1912 | 1912 |
| Object | DTLS1_BITMAP | DTLS1_BITMAP |

Code Snippet

File Name kbengine/d1_pkt.c

Method void dtls1_reset_seq_numbers(SSL *s, int rw)

```
....
1912.          memset(&(s->d1->next_bitmap), 0x00,
sizeof(DTLS1_BITMAP));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=220>

Status New

The size of the buffer used by dtls1_buffer_record in SSL3_BUFFER, at line 221 of kbengine/d1_pkt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dtls1_buffer_record passes to SSL3_BUFFER, at line 221 of kbengine/d1_pkt.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 261 | 261 |
| Object | SSL3_BUFFER | SSL3_BUFFER |

Code Snippet

File Name kbengine/d1_pkt.c

Method dtls1_buffer_record(SSL *s, record_pqueue *queue, unsigned char *priority)

```
....
261.          memset(&(s->s3->rbuf), 0, sizeof(SSL3_BUFFER));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=221>

Status New

The size of the buffer used by dtls1_buffer_record in SSL3_RECORD, at line 221 of kbengine/d1_pkt.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source

buffer that dtls1_buffer_record passes to SSL3_RECORD, at line 221 of kbengine/d1_pkt.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 262 | 262 |
| Object | SSL3_RECORD | SSL3_RECORD |

Code Snippet

File Name kbengine/d1_pkt.c

Method dtls1_buffer_record(SSL *s, record_pqueue *queue, unsigned char *priority)

```
....
262.      memset(&(s->s3->rrec), 0, sizeof(SSL3_RECORD));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=222>

Status New

The size of the buffer used by aesni_cbc_hmac_sha256_init_key in Namespace125441060, at line 116 of kbengine/e_aes_cbc_hmac_sha256.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that aesni_cbc_hmac_sha256_init_key passes to Namespace125441060, at line 116 of kbengine/e_aes_cbc_hmac_sha256.c, to overwrite the target buffer.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 124 | 124 |
| Object | Namespace125441060 | Namespace125441060 |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c

Method static int aesni_cbc_hmac_sha256_init_key(EVP_CIPHER_CTX *ctx,

```
....
124.      memset(&key->ks, 0, sizeof(key->ks.rd_key)),
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=223>

Status New

The size of the buffer used by curl_easy_reset in UserDefined, at line 1003 of kbengine/easy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that curl_easy_reset passes to UserDefined, at line 1003 of kbengine/easy.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 1013 | 1013 |
| Object | UserDefined | UserDefined |

Code Snippet

File Name kbengine/easy.c

Method void curl_easy_reset(struct Curl_easy *data)

```
....  
1013.     memset(&data->set, 0, sizeof(struct UserDefined));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=224>

Status New

The size of the buffer used by curl_easy_reset in Progress, at line 1003 of kbengine/easy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that curl_easy_reset passes to Progress, at line 1003 of kbengine/easy.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 1017 | 1017 |
| Object | Progress | Progress |

Code Snippet

File Name kbengine/easy.c

Method void curl_easy_reset(struct Curl_easy *data)

```
....  
1017.     memset(&data->progress, 0, sizeof(struct Progress));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=225>

Status New

The size of the buffer used by curl_easy_reset in auth, at line 1003 of kbengine/easy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that curl_easy_reset passes to auth, at line 1003 of kbengine/easy.c, to overwrite the target buffer.

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

| | | |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 1026 | 1026 |
| Object | auth | auth |

Code Snippet

File Name kbengine/easy.c

Method void curl_easy_reset(struct Curl_easy *data)

```
....
1026.     memset(&data->state.authhost, 0, sizeof(struct auth));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=226>

Status New

The size of the buffer used by curl_easy_reset in auth, at line 1003 of kbengine/easy.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that curl_easy_reset passes to auth, at line 1003 of kbengine/easy.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 1027 | 1027 |
| Object | auth | auth |

Code Snippet

File Name kbengine/easy.c

Method void curl_easy_reset(struct Curl_easy *data)

```
....
1027.     memset(&data->state.authproxy, 0, sizeof(struct auth));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=227>

Status New

The size of the buffer used by EVP_CIPHER_CTX_init in EVP_CIPHER_CTX, at line 80 of kbengine/evp_enc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EVP_CIPHER_CTX_init passes to EVP_CIPHER_CTX, at line 80 of kbengine/evp_enc.c, to overwrite the target buffer.

| | Source | Destination |
|------|--------------------|--------------------|
| File | kbengine/evp_enc.c | kbengine/evp_enc.c |

| | | |
|--------|----------------|----------------|
| Line | 82 | 82 |
| Object | EVP_CIPHER_CTX | EVP_CIPHER_CTX |

Code Snippet

File Name kbengine/evp_enc.c

Method void EVP_CIPHER_CTX_init(EVP_CIPHER_CTX *ctx)

```
....  
82.     memset(ctx, 0, sizeof(EVP_CIPHER_CTX));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=228>

Status New

The size of the buffer used by EVP_CIPHER_CTX_cleanup in EVP_CIPHER_CTX, at line 555 of kbengine/evp_enc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EVP_CIPHER_CTX_cleanup passes to EVP_CIPHER_CTX, at line 555 of kbengine/evp_enc.c, to overwrite the target buffer.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/evp_enc.c | kbengine/evp_enc.c |
| Line | 579 | 579 |
| Object | EVP_CIPHER_CTX | EVP_CIPHER_CTX |

Code Snippet

File Name kbengine/evp_enc.c

Method int EVP_CIPHER_CTX_cleanup(EVP_CIPHER_CTX *c)

```
....  
579.     memset(c, 0, sizeof(EVP_CIPHER_CTX));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=229>

Status New

The size of the buffer used by set_ciphers in ciphers, at line 302 of kbengine/gskit.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that set_ciphers passes to ciphers, at line 302 of kbengine/gskit.c, to overwrite the target buffer.

| | Source | Destination |
|------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 331 | 331 |

| | | |
|--------|---------|---------|
| Object | ciphers | ciphers |
|--------|---------|---------|

Code Snippet

File Name kbengine/gskit.c

Method static CURLcode set_ciphers(struct connectdata *conn,

```
....
331.     memset((char *) ciphers, 0, sizeof(ciphers));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=230>

Status New

The size of the buffer used by inetsocketpair in addr1, at line 526 of kbengine/gskit.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that inetsocketpair passes to addr1, at line 526 of kbengine/gskit.c, to overwrite the target buffer.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 539 | 539 |
| Object | addr1 | addr1 |

Code Snippet

File Name kbengine/gskit.c

Method inetsocketpair(int sv[2])

```
....
539.     memset((char *) &addr1, 0, sizeof(addr1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=231>

Status New

The size of the buffer used by curl_multi_add_handle in ->, at line 373 of kbengine/multi.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that curl_multi_add_handle passes to ->, at line 373 of kbengine/multi.c, to overwrite the target buffer.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 485 | 485 |
| Object | -> | -> |

Code Snippet

File Name kbengine/multi.c

Method CURLMcode curl_multi_add_handle(struct Curl_multi *multi,

```
....
485.     memset(&multi->timer_lastcall, 0, sizeof(multi-
>timer_lastcall));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=232>

Status New

The size of the buffer used by multi_socket in ->, at line 2541 of kbengine/multi.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multi_socket passes to ->, at line 2541 of kbengine/multi.c, to overwrite the target buffer.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 2638 | 2638 |
| Object | -> | -> |

Code Snippet

File Name kbengine/multi.c

Method static CURLMcode multi_socket(struct Curl_multi *multi,

```
....
2638.     memset(&multi->timer_lastcall, 0, sizeof(multi-
>timer_lastcall));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=233>

Status New

The size of the buffer used by nss_init_core in initparams, at line 1274 of kbengine/nss.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that nss_init_core passes to initparams, at line 1274 of kbengine/nss.c, to overwrite the target buffer.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 1281 | 1281 |
| Object | initparams | initparams |

Code Snippet

File Name kbengine/nss.c
Method static CURLcode nss_init_core(struct Curl_easy *data, const char *cert_dir)

```
....  
1281.      memset((void *) &initparams, '\\0', sizeof(initparams));
```

Buffer Overflow boundcpy WrongSizeParam\\Path 40:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=234>
Status New

The size of the buffer used by polarssl_connect_step1 in x509_crt, at line 219 of kbengine/polarssl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that polarssl_connect_step1 passes to x509_crt, at line 219 of kbengine/polarssl.c, to overwrite the target buffer.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 259 | 259 |
| Object | x509_crt | x509_crt |

Code Snippet

File Name kbengine/polarssl.c
Method polarssl_connect_step1(struct connectdata *conn,

```
....  
259.      memset(&BACKEND->cacert, 0, sizeof(x509_crt));
```

Buffer Overflow boundcpy WrongSizeParam\\Path 41:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=235>
Status New

The size of the buffer used by polarssl_connect_step1 in x509_crt, at line 219 of kbengine/polarssl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that polarssl_connect_step1 passes to x509_crt, at line 219 of kbengine/polarssl.c, to overwrite the target buffer.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 289 | 289 |
| Object | x509_crt | x509_crt |

Code Snippet

File Name kbengine/polarssl.c

Method polarssl_connect_step1(struct connectdata *conn,

```
....  
289.     memset(&BACKEND->clicert, 0, sizeof(x509_crt));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=236 |
| Status | New |

The size of the buffer used by polarssl_connect_step1 in x509_crl, at line 219 of kbengine/polarssl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that polarssl_connect_step1 passes to x509_crl, at line 219 of kbengine/polarssl.c, to overwrite the target buffer.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 328 | 328 |
| Object | x509_crl | x509_crl |

Code Snippet

File Name kbengine/polarssl.c
Method polarssl_connect_step1(struct connectdata *conn,

```
....  
328.     memset(&BACKEND->crl, 0, sizeof(x509_crl));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=237 |
| Status | New |

The size of the buffer used by myssh_statemach_act in ssh_conn, at line 546 of kbengine/ssh-libssh.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that myssh_statemach_act passes to ssh_conn, at line 546 of kbengine/ssh-libssh.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-----------------------|-----------------------|
| File | kbengine/ssh-libssh.c | kbengine/ssh-libssh.c |
| Line | 1881 | 1881 |
| Object | ssh_conn | ssh_conn |

Code Snippet

File Name kbengine/ssh-libssh.c
Method static CURLcode myssh_statemach_act(struct connectdata *conn, bool *block)

```
....  
1881.      memset(sshc, 0, sizeof(struct ssh_conn));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=238 |
| Status | New |

The size of the buffer used by operate_do in HdrCbData, at line 187 of kbengine/tool_operate.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that operate_do passes to HdrCbData, at line 187 of kbengine/tool_operate.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 213 | 213 |
| Object | HdrCbData | HdrCbData |

Code Snippet

File Name kbengine/tool_operate.c
Method static CURLcode operate_do(struct GlobalConfig *global,

```
....  
213.      memset(&hdrcbdata, 0, sizeof(struct HdrCbData));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=239 |
| Status | New |

The size of the buffer used by operate_do in OutStruct, at line 187 of kbengine/tool_operate.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that operate_do passes to OutStruct, at line 187 of kbengine/tool_operate.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 214 | 214 |
| Object | OutStruct | OutStruct |

Code Snippet

File Name kbengine/tool_operate.c
Method static CURLcode operate_do(struct GlobalConfig *global,

```
....  
214.      memset(&heads, 0, sizeof(struct OutStruct));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=240 |
| Status | New |

The size of the buffer used by operate_do in OutStruct, at line 187 of kbengine/tool_operate.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that operate_do passes to OutStruct, at line 187 of kbengine/tool_operate.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 510 | 510 |
| Object | OutStruct | OutStruct |

Code Snippet

File Name kbengine/tool_operate.c
Method static CURLcode operate_do(struct GlobalConfig *global,

```
....  
510.      memset(&outs, 0, sizeof(struct OutStruct));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=241 |
| Status | New |

The size of the buffer used by operate_do in OutStruct, at line 187 of kbengine/tool_operate.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that operate_do passes to OutStruct, at line 187 of kbengine/tool_operate.c, to overwrite the target buffer.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 1894 | 1894 |
| Object | OutStruct | OutStruct |

Code Snippet

File Name kbengine/tool_operate.c
Method static CURLcode operate_do(struct GlobalConfig *global,

```
.....  
1894.          memset(&outs, 0, sizeof(struct OutStruct));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=242 |
| Status | New |

The size of the buffer used by Curl_connect in SingleRequest, at line 4638 of kbengine/url.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_connect passes to SingleRequest, at line 4638 of kbengine/url.c, to overwrite the target buffer.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 4649 | 4649 |
| Object | SingleRequest | SingleRequest |

Code Snippet

File Name kbengine/url.c
Method CURLcode Curl_connect(struct Curl_easy *data,

```
.....  
4649.          memset(&data->req, 0, sizeof(struct SingleRequest));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=243 |
| Status | New |

The size of the buffer used by singlesocket in num, at line 2307 of kbengine/multi.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that singlesocket passes to num, at line 2307 of kbengine/multi.c, to overwrite the target buffer.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 2441 | 2441 |
| Object | num | num |

Code Snippet

File Name kbengine/multi.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,


```
.....
2441.      memcpy(data->sockets, socks, num*sizeof(curl_socket_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=244 |
| Status | New |

The size of the buffer used by singlesocket in curl_socket_t, at line 2307 of kbengine/multi.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that singlesocket passes to curl_socket_t, at line 2307 of kbengine/multi.c, to overwrite the target buffer.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 2441 | 2441 |
| Object | curl_socket_t | curl_socket_t |

Code Snippet

File Name kbengine/multi.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,

```
.....
2441.      memcpy(data->sockets, socks, num*sizeof(curl_socket_t));
```

Memory Leak

Query Path:

CPP\Cx\CPP Medium Threat\Memory Leak Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Memory Leak\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1182 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 2415 | 2415 |
| Object | req_buffer | req_buffer |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http(struct connectdata *conn, bool *done)

```
....  
2415.      req_buffer = Curl_add_buffer_init();
```

Memory Leak\Path 2:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1183>
Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 1904 | 1904 |
| Object | nickname | nickname |

Code Snippet

File Name kbengine/nss.c
Method static CURLcode nss_setup_connect(struct connectdata *conn, int sockindex)

```
....  
1904.      char *nickname = dup_nickname(data, SSL_SET_OPTION(cert));
```

Memory Leak\Path 3:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1184>
Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http2.c | kbengine/http2.c |
| Line | 2227 | 2227 |
| Object | dep | dep |

Code Snippet

File Name kbengine/http2.c
Method CURLcode Curl_http2_add_child(struct Curl_easy *parent,

```
....  
2227.      struct Curl_http2_dep *dep = calloc(1, sizeof(struct  
Curl_http2_dep));
```

Memory Leak\Path 4:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1185 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 397 | 397 |
| Object | wrap | wrap |

Code Snippet

File Name kbengine/nss.c

Method static CURLcode insert_wrapped_ptr(struct curl_llist *list, void *ptr)

```
....  
397.      struct ptr_list_wrap *wrap = malloc(sizeof(*wrap));
```

Memory Leak\Path 5:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1186 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1060 | 1060 |
| Object | filename | filename |

Code Snippet

File Name kbengine/cookie.c

Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....  
1060.      c->filename = strdup(file?file:"none"); /* copy the name just  
in case */
```

Memory Leak\Path 6:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1187 |
| Status | New |

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 49 | 49 |
| Object | real_path | real_path |

Code Snippet

File Name kbengine/curl_path.c

Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....  
49.         real_path = malloc(working_path_len + 1);
```

Memory Leak\Path 7:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1188>

Status New

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 63 | 63 |
| Object | real_path | real_path |

Code Snippet

File Name kbengine/curl_path.c

Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....  
63.         real_path = malloc(homelen + working_path_len + 1);
```

Memory Leak\Path 8:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1189>

Status New

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 79 | 79 |
| Object | real_path | real_path |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....  
79.         real_path = malloc(working_path_len + 1);
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1190>
Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 907 | 907 |
| Object | buffer | buffer |

Code Snippet

File Name kbengine/easy.c
Method struct Curl_easy *curl_easy_duphandle(struct Curl_easy *data)

```
....  
907.         outcurl->state.buffer = malloc(outcurl->set.buffer_size + 1);
```

Memory Leak\Path 10:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1191>
Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 911 | 911 |
| Object | headerbuff | headerbuff |

Code Snippet

File Name kbengine/easy.c
Method struct Curl_easy *curl_easy_duphandle(struct Curl_easy *data)

```
....  
911.         outcurl->state.headerbuff = malloc(HEADERSIZE);
```

Memory Leak\Path 11:

Severity Medium

| | |
|----------------|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1192 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 948 | 948 |
| Object | url | url |

Code Snippet

File Name kbengine/easy.c

Method struct Curl_easy *curl_easy_duphandle(struct Curl_easy *data)

```
....  
948.         outcurl->change.url = strdup(data->change.url);
```

Memory Leak\Path 12:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1193 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 955 | 955 |
| Object | referer | referer |

Code Snippet

File Name kbengine/easy.c

Method struct Curl_easy *curl_easy_duphandle(struct Curl_easy *data)

```
....  
955.         outcurl->change.referer = strdup(data->change.referer);
```

Memory Leak\Path 13:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1194 |
| Status | New |

| | Source | Destination |
|------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |

| | | |
|--------|------|------|
| Line | 4387 | 4387 |
| Object | ftp | ftp |

Code Snippet

File Name kbengine/ftp.c

Method static CURLcode ftp_setup_connection(struct connectdata *conn)

```
....  
4387.      conn->data->req.protop = ftp = malloc(sizeof(struct FTP));
```

Memory Leak\Path 14:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1195>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 1866 | 1866 |
| Object | newhost | newhost |

Code Snippet

File Name kbengine/ftp.c

Method static CURLcode ftp_state_pasv_resp(struct connectdata *conn,

```
....  
1866.      ftpc->newhost = strdup(control_address(conn));
```

Memory Leak\Path 15:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1196>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 1915 | 1915 |
| Object | newhost | newhost |

Code Snippet

File Name kbengine/ftp.c

Method static CURLcode ftp_state_pasv_resp(struct connectdata *conn,

```
.....
1915.          ftpc->newhost = strdup(control_address(conn));
```

Memory Leak\Path 16:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1197 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 1997 | 1997 |
| Object | secondaryhostname | secondaryhostname |

Code Snippet

File Name kbengine/ftp.c
Method static CURLcode ftp_state_pasv_resp(struct connectdata *conn,

```
.....
1997.      conn->secondaryhostname = strdup(ftp->newhost);
```

Memory Leak\Path 17:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1198 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 3217 | 3217 |
| Object | prevpath | prevpath |

Code Snippet

File Name kbengine/ftp.c
Method static CURLcode ftp_done(struct connectdata *conn, CURLcode status,

```
.....
3217.          ftpc->prevpath = strdup("");
```

Memory Leak\Path 18:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1199 |

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1199](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1199)

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 3711 | 3711 |
| Object | pattern | pattern |

Code Snippet

File Name kbengine/ftp.c

Method static CURLcode init_wc_data(struct connectdata *conn)

```
....  
3711.          wildcard->pattern = strdup(last_slash);
```

Memory Leak\Path 19:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1200>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 3718 | 3718 |
| Object | pattern | pattern |

Code Snippet

File Name kbengine/ftp.c

Method static CURLcode init_wc_data(struct connectdata *conn)

```
....  
3718.          wildcard->pattern = strdup(path);
```

Memory Leak\Path 20:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1201>

Status New

| | Source | Destination |
|------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 3760 | 3760 |

| | | |
|--------|------|------|
| Object | path | path |
|--------|------|------|

Code Snippet

File Name kbengine/ftp.c

Method static CURLcode init_wc_data(struct connectdata *conn)

```
....
3760.    wildcard->path = strdup(conn->data->state.path);
```

Memory Leak\Path 21:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1202>

Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 333 | 333 |
| Object | buf | buf |

Code Snippet

File Name kbengine/gskit.c

Method static CURLcode set_ciphers(struct connectdata *conn,

```
....
333.    ciphers[i].buf = malloc(1);
```

Memory Leak\Path 22:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1203>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |
| Line | 931 | 931 |
| Object | buff1 | buff1 |

Code Snippet

File Name kbengine/gtls.c

Method static CURLcode pkp_pin_peer_pubkey(struct Curl_easy *data,

```
....
931.      buff1 = malloc(len1);
```

Memory Leak\Path 23:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1204 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 3875 | 3875 |
| Object | newurl | newurl |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http_readwrite_headers(struct Curl_easy *data,

```
....
3875.      data->req.newurl = strdup(data->req.location); /* clone
*/
```

Memory Leak\Path 24:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1205 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 164 | 164 |
| Object | http | http |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http_setup_conn(struct connectdata *conn)

```
....
164.      http = calloc(1, sizeof(struct HTTP));
```

Memory Leak\Path 25:

| | |
|--------------|-----------|
| Severity | Medium |
| Result State | To Verify |

| | |
|----------------|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1206 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 249 | 249 |
| Object | value | value |

Code Snippet

File Name kbengine/http.c

Method char *Curl_copy_header_value(const char *header)

```
....  
249.     value = malloc(len + 1);
```

Memory Leak\Path 26:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1207 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 544 | 544 |
| Object | newurl | newurl |

Code Snippet

File Name kbengine/http.c

Method CURLcode Curl_http_auth_act(struct connectdata *conn)

```
....  
544.     data->req.newurl = strdup(data->change.url); /* clone URL */
```

Memory Leak\Path 27:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1208 |
| Status | New |

| | Source | Destination |
|------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |

| | | |
|--------|--------|--------|
| Line | 565 | 565 |
| Object | newurl | newurl |

Code Snippet

File Name kbengine/http.c

Method CURLcode Curl_http_auth_act(struct connectdata *conn)

```
....  
565.          data->req.newurl = strdup(data->change.url); /* clone URL */
```

Memory Leak\Path 28:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1209>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 836 | 836 |
| Object | newurl | newurl |

Code Snippet

File Name kbengine/http.c

Method CURLcode Curl_http_input_auth(struct connectdata *conn, bool proxy,

```
....  
836.          data->req.newurl = strdup(data->change.url);
```

Memory Leak\Path 29:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1210>

Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 882 | 882 |
| Object | challenge_header | challenge_header |

Code Snippet

File Name kbengine/http.c

Method CURLcode Curl_http_input_auth(struct connectdata *conn, bool proxy,

```
.....  
882.                conn->challenge_header = strdup(auth);
```

Memory Leak\Path 30:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1211 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 1936 | 1936 |
| Object | first_host | first_host |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http(struct connectdata *conn, bool *done)

```
.....  
1936.                data->state.first_host = strdup(conn->host.name);
```

Memory Leak\Path 31:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1212 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 2233 | 2233 |
| Object | newurl | newurl |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http(struct connectdata *conn, bool *done)

```
.....  
2233.                newurl = malloc(urllen + newlen - currlen + 1);
```

Memory Leak\Path 32:

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

| | |
|--------|--|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1213 |
| Status | New |

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http2.c | kbengine/http2.c |
| Line | 925 | 925 |
| Object | push_headers | push_headers |

Code Snippet

File Name kbengine/http2.c

Method static int on_header(nghttp2_session *session, const nghttp2_frame *frame,

```
....
925.         stream->push_headers = malloc(stream->push_headers_alloc *
```

Memory Leak\Path 33:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1214>

Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http2.c | kbengine/http2.c |
| Line | 1142 | 1142 |
| Object | inbuf | inbuf |

Code Snippet

File Name kbengine/http2.c

Method CURLcode Curl_http2_init(struct connectdata *conn)

```
....
1142.         conn->proto.httpc.inbuf = malloc(H2_BUFSIZE);
```

Memory Leak\Path 34:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1215>

Status New

| | Source | Destination |
|------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 2091 | 2091 |

| | | |
|--------|---------------|---------------|
| Object | custom_params | custom_params |
|--------|---------------|---------------|

Code Snippet

File Name kbengine/imap.c

Method static CURLcode imap_parse_custom_request(struct connectdata *conn)

```
....
2091.         imap->custom_params = strdup(params);
```

Memory Leak\Path 35:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1216>

Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1057 | 1057 |
| Object | mailbox_uidvalidity | mailbox_uidvalidity |

Code Snippet

File Name kbengine/imap.c

Method static CURLcode imap_state_select_resp(struct connectdata *conn, int imapcode,

```
....
1057.         imapc->mailbox_uidvalidity = strdup(tmp);
```

Memory Leak\Path 36:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1217>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1069 | 1069 |
| Object | mailbox | mailbox |

Code Snippet

File Name kbengine/imap.c

Method static CURLcode imap_state_select_resp(struct connectdata *conn, int imapcode,


```
.....  
1069.      imapc->mailbox = strdup(imap->mailbox);
```

Memory Leak\Path 37:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1218 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1377 | 1377 |
| Object | protop | protop |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_init(struct connectdata *conn)

```
.....  
1377.      imap = data->req.protop = calloc(sizeof(struct IMAP), 1);
```

Memory Leak\Path 38:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1219 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1813 | 1813 |
| Object | newstr | newstr |

Code Snippet

File Name kbengine/imap.c
Method static char *imap_atom(const char *str, bool escape_only)

```
.....  
1813.      newstr = (char *) malloc((newlen + 1) * sizeof(char));
```

Memory Leak\Path 39:

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

| | |
|--------|--|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1220 |
| Status | New |

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/mprintf.c | kbengine/mprintf.c |
| Line | 1035 | 1035 |
| Object | buffer | buffer |

Code Snippet

File Name kbengine/mprintf.c

Method static int alloc_addbyter(int output, FILE *data)

```
....  
1035.      infop->buffer = malloc(32);
```

Memory Leak\Path 40:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1221>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/pop3.c | kbengine/pop3.c |
| Line | 636 | 636 |
| Object | apoptimestamp | apoptimestamp |

Code Snippet

File Name kbengine/pop3.c

Method static CURLcode pop3_state_servergreet_resp(struct connectdata *conn,

```
....  
636.      pop3c->apoptimestamp = (char *)calloc(1, timestamplen +  
1);
```

Memory Leak\Path 41:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1222>

Status New

| | Source | Destination |
|------|-----------------|-----------------|
| File | kbengine/pop3.c | kbengine/pop3.c |

| | | |
|--------|--------|--------|
| Line | 1045 | 1045 |
| Object | protop | protop |

Code Snippet

File Name kbengine/pop3.c

Method static CURLcode pop3_init(struct connectdata *conn)

```
....
1045.     pop3 = data->req.protop = calloc(sizeof(struct POP3), 1);
```

Memory Leak\Path 42:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1223>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/rtsp.c | kbengine/rtsp.c |
| Line | 134 | 134 |
| Object | rtsp | rtsp |

Code Snippet

File Name kbengine/rtsp.c

Method static CURLcode rtsp_setup_connection(struct connectdata *conn)

```
....
134.     conn->data->req.protop = rtsp = calloc(1, sizeof(struct RTSP));
```

Memory Leak\Path 43:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1224>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/rtsp.c | kbengine/rtsp.c |
| Line | 707 | 707 |
| Object | scratch | scratch |

Code Snippet

File Name kbengine/rtsp.c

Method static CURLcode rtsp_rtp_readwrite(struct Curl_easy *data,

```
....  
707.      scratch = malloc(rtp_dataleft);
```

Memory Leak\Path 44:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1225 |
| Status | New |

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 650 | 650 |
| Object | cred | cred |

Code Snippet

File Name kbengine/schannel.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....  
650.      BACKEND->cred = (struct curl_schannel_cred *)
```

Memory Leak\Path 45:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1226 |
| Status | New |

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 758 | 758 |
| Object | ctxt | ctxt |

Code Snippet

File Name kbengine/schannel.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....  
758.      BACKEND->ctxt = (struct curl_schannel_ctxt *)
```

Memory Leak\Path 46:

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

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1227](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1227)

Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 855 | 855 |
| Object | decdata_buffer | decdata_buffer |

Code Snippet

File Name kbengine/schannel.c

Method schannel_connect_step2(struct connectdata *conn, int sockindex)

```
....  
855.         BACKEND->decdata_buffer = malloc(BACKEND->decdata_length);
```

Memory Leak\Path 47:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1228>

Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 867 | 867 |
| Object | encdata_buffer | encdata_buffer |

Code Snippet

File Name kbengine/schannel.c

Method schannel_connect_step2(struct connectdata *conn, int sockindex)

```
....  
867.         BACKEND->encdata_buffer = malloc(BACKEND->encdata_length);
```

Memory Leak\Path 48:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1229>

Status New

| | Source | Destination |
|------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 1363 | 1363 |

| | | |
|--------|------|------|
| Object | data | data |
|--------|------|------|

Code Snippet

File Name kbengine/schannel.c

Method schannel_send(struct connectdata *conn, int sockindex,

```
....  
1363.     data = (unsigned char *) malloc(data_len);
```

Memory Leak\Path 49:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1230>

Status New

| | Source | Destination |
|--------|----------------------------|----------------------------|
| File | kbengine/schannel_verify.c | kbengine/schannel_verify.c |
| Line | 143 | 143 |
| Object | ca_file_buffer | ca_file_buffer |

Code Snippet

File Name kbengine/schannel_verify.c

Method static CURLcode add_certs_to_store(HCERTSTORE trust_store,

```
....  
143.     ca_file_buffer = (char *)malloc(ca_file_bufsize + 1);
```

Memory Leak\Path 50:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1231>

Status New

| | Source | Destination |
|--------|----------------------------|----------------------------|
| File | kbengine/schannel_verify.c | kbengine/schannel_verify.c |
| Line | 321 | 321 |
| Object | cert_hostname_buff | cert_hostname_buff |

Code Snippet

File Name kbengine/schannel_verify.c

Method static CURLcode verify_host(struct Curl_easy *data,

```
....
321.      cert_hostname_buff = (LPTSTR)malloc(len * sizeof(TCHAR));
```

MemoryFree on StackVariable

Query Path:

CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

[Description](#)

MemoryFree on StackVariable\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=426 |
| Status | New |

Calling free() (line 1529) on a variable that was not dynamically allocated (line 1529) in file kbengine/cookie.c may result with a crash.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1552 | 1552 |
| Object | line | line |

Code Snippet

File Name kbengine/cookie.c
Method static struct curl_slist *cookie_list(struct Curl_easy *data)

```
....
1552.      free(line);
```

MemoryFree on StackVariable\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=427 |
| Status | New |

Calling free() (line 32) on a variable that was not dynamically allocated (line 32) in file kbengine/curl_path.c may result with a crash.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 51 | 51 |
| Object | working_path | working_path |

Code Snippet

File Name kbengine/curl_path.c

Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....  
51.            free(working_path);
```

MemoryFree on StackVariable\Path 3:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=428 |
| Status | New |

Calling free() (line 32) on a variable that was not dynamically allocated (line 32) in file kbengine/curl_path.c may result with a crash.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 65 | 65 |
| Object | working_path | working_path |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....  
65.            free(working_path);
```

MemoryFree on StackVariable\Path 4:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=429 |
| Status | New |

Calling free() (line 32) on a variable that was not dynamically allocated (line 32) in file kbengine/curl_path.c may result with a crash.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 81 | 81 |
| Object | working_path | working_path |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,


```
....
81.      free(working_path);
```

MemoryFree on StackVariable\Path 5:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=430 |
| Status | New |

Calling free() (line 32) on a variable that was not dynamically allocated (line 32) in file kbengine/curl_path.c may result with a crash.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 88 | 88 |
| Object | working_path | working_path |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....
88.      free(working_path);
```

MemoryFree on StackVariable\Path 6:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=431 |
| Status | New |

Calling free() (line 410) on a variable that was not dynamically allocated (line 410) in file kbengine/curl_sasl.c may result with a crash.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_sasl.c | kbengine/curl_sasl.c |
| Line | 477 | 477 |
| Object | chlg | chlg |

Code Snippet

File Name kbengine/curl_sasl.c
Method CURLcode Curl_sasl_continue(struct SASL *sasl, struct connectdata *conn,

```
....  
477.         free(chlg);
```

MemoryFree on StackVariable\Path 7:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=432 |
| Status | New |

Calling free() (line 253) on a variable that was not dynamically allocated (line 253) in file kbengine/curl_sasl.c may result with a crash.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_sasl.c | kbengine/curl_sasl.c |
| Line | 389 | 389 |
| Object | resp | resp |

Code Snippet

File Name kbengine/curl_sasl.c
Method CURLcode Curl_sasl_start(struct SASL *sasl, struct connectdata *conn,

```
....  
389.         free(resp);
```

MemoryFree on StackVariable\Path 8:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=433 |
| Status | New |

Calling free() (line 253) on a variable that was not dynamically allocated (line 253) in file kbengine/curl_sasl.c may result with a crash.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_sasl.c | kbengine/curl_sasl.c |
| Line | 400 | 400 |
| Object | resp | resp |

Code Snippet

File Name kbengine/curl_sasl.c
Method CURLcode Curl_sasl_start(struct SASL *sasl, struct connectdata *conn,

```
.....
400.      free (resp);
```

MemoryFree on StackVariable\Path 9:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=434 |
| Status | New |

Calling free() (line 94) on a variable that was not dynamically allocated (line 94) in file kbengine/dict.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/dict.c | kbengine/dict.c |
| Line | 122 | 122 |
| Object | newp | newp |

Code Snippet

File Name kbengine/dict.c
Method static char *unescape_word(struct Curl_easy *data, const char *inputbuff)

```
.....
122.      free (newp);
```

MemoryFree on StackVariable\Path 10:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=435 |
| Status | New |

Calling free() (line 1443) on a variable that was not dynamically allocated (line 1443) in file kbengine/ftp.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 1489 | 1489 |
| Object | lstArg | lstArg |

Code Snippet

File Name kbengine/ftp.c
Method static CURLcode ftp_state_list(struct connectdata *conn)

```
.....  
1489.      free(lstArg);
```

MemoryFree on StackVariable\Path 11:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=436 |
| Status | New |

Calling free() (line 1443) on a variable that was not dynamically allocated (line 1443) in file kbengine/ftp.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 1495 | 1495 |
| Object | lstArg | lstArg |

Code Snippet

File Name kbengine/ftp.c
Method static CURLcode ftp_state_list(struct connectdata *conn)

```
.....  
1495.      free(lstArg);
```

MemoryFree on StackVariable\Path 12:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=437 |
| Status | New |

Calling free() (line 1443) on a variable that was not dynamically allocated (line 1443) in file kbengine/ftp.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 1496 | 1496 |
| Object | cmd | cmd |

Code Snippet

File Name kbengine/ftp.c
Method static CURLcode ftp_state_list(struct connectdata *conn)

```
....  
1496.      free(cmd);
```

MemoryFree on StackVariable\Path 13:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=438 |
| Status | New |

Calling free() (line 3133) on a variable that was not dynamically allocated (line 3133) in file kbengine/ftp.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 3218 | 3218 |
| Object | path | path |

Code Snippet

File Name kbengine/ftp.c
Method static CURLcode ftp_done(struct connectdata *conn, CURLcode status,

```
....  
3218.      free(path);
```

MemoryFree on StackVariable\Path 14:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=439 |
| Status | New |

Calling free() (line 3133) on a variable that was not dynamically allocated (line 3133) in file kbengine/ftp.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 3225 | 3225 |
| Object | path | path |

Code Snippet

File Name kbengine/ftp.c
Method static CURLcode ftp_done(struct connectdata *conn, CURLcode status,

```
.....
3225.      free(path);
```

MemoryFree on StackVariable\Path 15:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=440 |
| Status | New |

Calling free() (line 3687) on a variable that was not dynamically allocated (line 3687) in file kbengine/ftp.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 3692 | 3692 |
| Object | ftppwc | ftppwc |

Code Snippet

File Name kbengine/ftp.c
Method static void wc_data_dtor(void *ptr)

```
.....
3692.      free(ftppwc);
```

MemoryFree on StackVariable\Path 16:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=441 |
| Status | New |

Calling free() (line 4097) on a variable that was not dynamically allocated (line 4097) in file kbengine/ftp.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 4280 | 4280 |
| Object | path | path |

Code Snippet

File Name kbengine/ftp.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
.....
4280.          free(path);
```

MemoryFree on StackVariable\Path 17:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=442 |
| Status | New |

Calling free() (line 3095) on a variable that was not dynamically allocated (line 3095) in file kbengine/http.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 3699 | 3699 |
| Object | contenttype | contenttype |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http_readwrite_headers(struct Curl_easy *data,

```
.....
3699.          free(contenttype);
```

MemoryFree on StackVariable\Path 18:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=443 |
| Status | New |

Calling free() (line 3095) on a variable that was not dynamically allocated (line 3095) in file kbengine/http.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 3715 | 3715 |
| Object | server_name | server_name |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http_readwrite_headers(struct Curl_easy *data,

```
....  
3715.          free(server_name);
```

MemoryFree on StackVariable\Path 19:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=444 |
| Status | New |

Calling free() (line 3095) on a variable that was not dynamically allocated (line 3095) in file kbengine/http.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 3855 | 3855 |
| Object | auth | auth |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http_readwrite_headers(struct Curl_easy *data,

```
....  
3855.          free(auth);
```

MemoryFree on StackVariable\Path 20:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=445 |
| Status | New |

Calling free() (line 3095) on a variable that was not dynamically allocated (line 3095) in file kbengine/http.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 3869 | 3869 |
| Object | location | location |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http_readwrite_headers(struct Curl_easy *data,


```
.....  
3869.          free(location);
```

MemoryFree on StackVariable\Path 21:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=446 |
| Status | New |

Calling free() (line 265) on a variable that was not dynamically allocated (line 265) in file kbengine/http.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 304 | 304 |
| Object | authorization | authorization |

Code Snippet

File Name kbengine/http.c
Method static CURLcode http_output_basic(struct connectdata *conn, bool proxy)

```
.....  
304.          free(authorization);
```

MemoryFree on StackVariable\Path 22:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=447 |
| Status | New |

Calling free() (line 265) on a variable that was not dynamically allocated (line 265) in file kbengine/http.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 311 | 311 |
| Object | out | out |

Code Snippet

File Name kbengine/http.c
Method static CURLcode http_output_basic(struct connectdata *conn, bool proxy)

```
....  
311.      free(out);
```

MemoryFree on StackVariable\Path 23:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=448 |
| Status | New |

Calling free() (line 1268) on a variable that was not dynamically allocated (line 1268) in file kbengine/http.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 1278 | 1278 |
| Object | s | s |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_add_bufferf(Curl_send_buffer *in, const char *fmt, ...)

```
....  
1278.      free(s);
```

MemoryFree on StackVariable\Path 24:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=449 |
| Status | New |

Calling free() (line 1867) on a variable that was not dynamically allocated (line 1867) in file kbengine/http.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 2056 | 2056 |
| Object | cptr | cptr |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http(struct connectdata *conn, bool *done)

```
.....
2056.          free(cpPtr);
```

MemoryFree on StackVariable\Path 25:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=450 |
| Status | New |

Calling free() (line 1867) on a variable that was not dynamically allocated (line 1867) in file kbengine/http.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 2152 | 2152 |
| Object | cookiehost | cookiehost |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http(struct connectdata *conn, bool *done)

```
.....
2152.          free(cookiehost);
```

MemoryFree on StackVariable\Path 26:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=451 |
| Status | New |

Calling free() (line 1188) on a variable that was not dynamically allocated (line 1188) in file kbengine/http2.c may result with a crash.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http2.c | kbengine/http2.c |
| Line | 1224 | 1224 |
| Object | base64 | base64 |

Code Snippet

File Name kbengine/http2.c
Method CURLcode Curl_http2_request_upgrade(Curl_send_buffer *req,

```
.....
1224.      free(base64);
```

MemoryFree on StackVariable\Path 27:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=452 |
| Status | New |

Calling free() (line 2263) on a variable that was not dynamically allocated (line 2263) in file kbengine/http2.c may result with a crash.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http2.c | kbengine/http2.c |
| Line | 2283 | 2283 |
| Object | data | data |

Code Snippet

File Name kbengine/http2.c
Method void Curl_http2_remove_child(struct Curl_easy *parent, struct Curl_easy *child)

```
.....
2283.      free(data);
```

MemoryFree on StackVariable\Path 28:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=453 |
| Status | New |

Calling free() (line 490) on a variable that was not dynamically allocated (line 490) in file kbengine/imap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 512 | 512 |
| Object | user | user |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_perform_login(struct connectdata *conn)

```
.....  
512.      free(user);
```

MemoryFree on StackVariable\Path 29:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=454 |
| Status | New |

Calling free() (line 490) on a variable that was not dynamically allocated (line 490) in file kbengine/imap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 513 | 513 |
| Object | passwd | passwd |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_perform_login(struct connectdata *conn)

```
.....  
513.      free(passwd);
```

MemoryFree on StackVariable\Path 30:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=455 |
| Status | New |

Calling free() (line 642) on a variable that was not dynamically allocated (line 642) in file kbengine/imap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 668 | 668 |
| Object | mailbox | mailbox |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_perform_select(struct connectdata *conn)

```
....  
668.      free(mailbox);
```

MemoryFree on StackVariable\Path 31:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=456 |
| Status | New |

Calling free() (line 716) on a variable that was not dynamically allocated (line 716) in file kbengine/imap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 773 | 773 |
| Object | mailbox | mailbox |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_perform_append(struct connectdata *conn)

```
....  
773.      free(mailbox);
```

MemoryFree on StackVariable\Path 32:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=457 |
| Status | New |

Calling free() (line 1727) on a variable that was not dynamically allocated (line 1727) in file kbengine/imap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1753 | 1753 |
| Object | taggedfmt | taggedfmt |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_sendf(struct connectdata *conn, const char *fmt, ...)

```
.....  
1753.      free (taggedfmt);
```

MemoryFree on StackVariable\Path 33:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=458 |
| Status | New |

Calling free() (line 1941) on a variable that was not dynamically allocated (line 1941) in file kbengine/imap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1995 | 1995 |
| Object | name | name |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_parse_url_path(struct connectdata *conn)

```
.....  
1995.      free (name);
```

MemoryFree on StackVariable\Path 34:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=459 |
| Status | New |

Calling free() (line 1941) on a variable that was not dynamically allocated (line 1941) in file kbengine/imap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 2034 | 2034 |
| Object | name | name |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_parse_url_path(struct connectdata *conn)

```
.....
2034.          free(name);
```

MemoryFree on StackVariable\Path 35:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=460 |
| Status | New |

Calling free() (line 1941) on a variable that was not dynamically allocated (line 1941) in file kbengine/imap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 2035 | 2035 |
| Object | value | value |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_parse_url_path(struct connectdata *conn)

```
.....
2035.          free(value);
```

MemoryFree on StackVariable\Path 36:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=461 |
| Status | New |

Calling free() (line 1941) on a variable that was not dynamically allocated (line 1941) in file kbengine/imap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 2040 | 2040 |
| Object | name | name |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_parse_url_path(struct connectdata *conn)


```
.....
2040.      free(name);
```

MemoryFree on StackVariable\Path 37:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=462 |
| Status | New |

Calling free() (line 1941) on a variable that was not dynamically allocated (line 1941) in file kbengine/imap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 2041 | 2041 |
| Object | value | value |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_parse_url_path(struct connectdata *conn)

```
.....
2041.      free(value);
```

MemoryFree on StackVariable\Path 38:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=463 |
| Status | New |

Calling free() (line 146) on a variable that was not dynamically allocated (line 146) in file kbengine/krb5.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/krb5.c | kbengine/krb5.c |
| Line | 205 | 205 |
| Object | stringp | stringp |

Code Snippet

File Name kbengine/krb5.c
Method krb5_auth(void *app_data, struct connectdata *conn)

```
....
205.         free(stringp);
```

MemoryFree on StackVariable\Path 39:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=464 |
| Status | New |

Calling free() (line 146) on a variable that was not dynamically allocated (line 146) in file kbengine/krb5.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/krb5.c | kbengine/krb5.c |
| Line | 267 | 267 |
| Object | p | p |

Code Snippet

File Name kbengine/krb5.c
Method krb5_auth(void *app_data, struct connectdata *conn)

```
....
267.         free(p);
```

MemoryFree on StackVariable\Path 40:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=465 |
| Status | New |

Calling free() (line 253) on a variable that was not dynamically allocated (line 253) in file kbengine/ldap.c may result with a crash.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/ldap.c | kbengine/ldap.c |
| Line | 648 | 648 |
| Object | val_b64 | val_b64 |

Code Snippet

File Name kbengine/ldap.c
Method

```
.....  
648.                                     val_b64_sz);
```

MemoryFree on StackVariable\Path 41:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=466 |
| Status | New |

Calling free() (line 256) on a variable that was not dynamically allocated (line 256) in file kbengine/multi.c may result with a crash.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 260 | 260 |
| Object | p | p |

Code Snippet

File Name kbengine/multi.c
Method static void sh_freeentry(void *freethis)

```
.....  
260.     free(p);
```

MemoryFree on StackVariable\Path 42:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=467 |
| Status | New |

Calling free() (line 1327) on a variable that was not dynamically allocated (line 1327) in file kbengine/multi.c may result with a crash.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 1749 | 1749 |
| Object | newurl | newurl |

Code Snippet

File Name kbengine/multi.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
.....  
1749.                free(newurl);
```

MemoryFree on StackVariable\Path 43:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=468 |
| Status | New |

Calling free() (line 1327) on a variable that was not dynamically allocated (line 1327) in file kbengine/multi.c may result with a crash.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 1981 | 1981 |
| Object | newurl | newurl |

Code Snippet

File Name kbengine/multi.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
.....  
1981.                free(newurl);
```

MemoryFree on StackVariable\Path 44:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=469 |
| Status | New |

Calling free() (line 1327) on a variable that was not dynamically allocated (line 1327) in file kbengine/multi.c may result with a crash.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 2003 | 2003 |
| Object | newurl | newurl |

Code Snippet

File Name kbengine/multi.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....  
2003.                free(newurl);
```

MemoryFree on StackVariable\Path 45:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=470 |
| Status | New |

Calling free() (line 1327) on a variable that was not dynamically allocated (line 1327) in file kbengine/multi.c may result with a crash.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 2018 | 2018 |
| Object | newurl | newurl |

Code Snippet

File Name kbengine/multi.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....  
2018.                free(newurl);
```

MemoryFree on StackVariable\Path 46:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=471 |
| Status | New |

Calling free() (line 409) on a variable that was not dynamically allocated (line 409) in file kbengine/nss.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 429 | 429 |
| Object | slot_name | slot_name |

Code Snippet

File Name kbengine/nss.c
Method static CURLcode nss_create_object(struct ssl_connect_data *connssl,

```
.....
429.      free(slot_name);
```

MemoryFree on StackVariable\Path 47:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=472 |
| Status | New |

Calling free() (line 473) on a variable that was not dynamically allocated (line 473) in file kbengine/nss.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 479 | 479 |
| Object | wrap | wrap |

Code Snippet

File Name kbengine/nss.c
Method static void nss_destroy_object(void *user, void *ptr)

```
.....
479.      free(wrap);
```

MemoryFree on StackVariable\Path 48:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=473 |
| Status | New |

Calling free() (line 483) on a variable that was not dynamically allocated (line 483) in file kbengine/nss.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 489 | 489 |
| Object | wrap | wrap |

Code Snippet

File Name kbengine/nss.c
Method static void nss_destroy_crl_item(void *user, void *ptr)

```
.....
489.      free(wrap);
```

MemoryFree on StackVariable\Path 49:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=474 |
| Status | New |

Calling free() (line 492) on a variable that was not dynamically allocated (line 492) in file kbengine/nss.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 522 | 522 |
| Object | nickname | nickname |

Code Snippet

File Name kbengine/nss.c
Method static CURLcode nss_load_cert(struct ssl_connect_data *ssl,

```
.....
522.      free(nickname);
```

MemoryFree on StackVariable\Path 50:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=475 |
| Status | New |

Calling free() (line 1230) on a variable that was not dynamically allocated (line 1230) in file kbengine/nss.c may result with a crash.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 1244 | 1244 |
| Object | config_string | config_string |

Code Snippet

File Name kbengine/nss.c
Method static CURLcode nss_load_module(SECMODModule **pmod, const char *library,

```
....
1244.      free(config_string);
```

Wrong Size t Allocation

Query Path:

CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0

[Description](#)

Wrong Size t Allocation\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=494 |
| Status | New |

The function fullPathLength in kbengine/curl_path.c at line 113 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 131 | 131 |
| Object | fullPathLength | fullPathLength |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_get_pathname(const char **cpp, char **path, char *homedir)

```
....
131.      *path = malloc(fullPathLength);
```

Wrong Size t Allocation\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=495 |
| Status | New |

The function alloc in kbengine/escape.c at line 79 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/escape.c | kbengine/escape.c |
| Line | 96 | 96 |
| Object | alloc | alloc |

Code Snippet

File Name kbengine/escape.c
Method char *curl_easy_escape(struct Curl_easy *data, const char *string,

```
....  
96.     ns = malloc(alloc);
```

Wrong Size t Allocation\Path 3:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=496>
Status New

The function alloc in kbengine/escape.c at line 145 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/escape.c | kbengine/escape.c |
| Line | 151 | 151 |
| Object | alloc | alloc |

Code Snippet

File Name kbengine/escape.c
Method CURLcode Curl_urldecode(struct Curl_easy *data,

```
....  
151.     char *ns = malloc(alloc);
```

Wrong Size t Allocation\Path 4:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=497>
Status New

The function len1 in kbengine/gtls.c at line 898 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |
| Line | 931 | 931 |
| Object | len1 | len1 |

Code Snippet

File Name kbengine/gtls.c
Method static CURLcode pkp_pin_peer_pubkey(struct Curl_easy *data,

```
....  
931.      buff1 = malloc(len1);
```

Wrong Size t Allocation\Path 5:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=498 |
| Status | New |

The function connect_idsize in kbengine/gtls.c at line 959 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |
| Line | 1426 | 1426 |
| Object | connect_idsize | connect_idsize |

Code Snippet

File Name kbengine/gtls.c
Method gtls_connect_step3(struct connectdata *conn,

```
....  
1426.      connect_sessionid = malloc(connect_idsize); /* get a buffer  
for it */
```

Wrong Size t Allocation\Path 6:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=499 |
| Status | New |

The function new_size in kbengine/http.c at line 1290 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 1321 | 1321 |
| Object | new_size | new_size |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_add_buffer(Curl_send_buffer *in, const void *inptr, size_t size)

```
....
1321.         new_rb = malloc(new_size);
```

Wrong Size t Allocation\Path 7:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=500 |
| Status | New |

The function bufsize in kbengine/mbedtls.c at line 534 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/mbedtls.c | kbengine/mbedtls.c |
| Line | 602 | 602 |
| Object | bufsize | bufsize |

Code Snippet

File Name kbengine/mbedtls.c
Method mbed_connect_step2(struct connectdata *conn,

```
....
602.         char *buffer = malloc(bufsize);
```

Wrong Size t Allocation\Path 8:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=501 |
| Status | New |

The function data_len in kbengine/schannel.c at line 1363 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 1363 | 1363 |
| Object | data_len | data_len |

Code Snippet

File Name kbengine/schannel.c
Method schannel_send(struct connectdata *conn, int sockindex,

```
....
1363.      data = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 9:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=502 |
| Status | New |

The function buflen in kbengine/sds.c at line 360 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 366 | 366 |
| Object | buflen | buflen |

Code Snippet

File Name kbengine/sds.c
Method sds sdscatvprintf(sds s, const char *fmt, va_list ap) {

```
....
366.      buf = malloc(buflen);
```

Wrong Size t Allocation\Path 10:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=503 |
| Status | New |

The function outlen in kbengine/vtls.c at line 685 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |
| Line | 698 | 698 |
| Object | outlen | outlen |

Code Snippet

File Name kbengine/vtls.c
Method CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....  
698.      output = malloc(outlen);
```

Wrong Size t Allocation\Path 11:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=504 |
| Status | New |

The function pinkeylen in kbengine/vtls.c at line 805 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |
| Line | 855 | 855 |
| Object | pinkeylen | pinkeylen |

Code Snippet

File Name kbengine/vtls.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....  
855.      pinkeycopy = malloc(pinkeylen);
```

Wrong Size t Allocation\Path 12:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=505 |
| Status | New |

The function newsize in kbengine/http.c at line 3038 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 3038 | 3038 |
| Object | newsize | newsize |

Code Snippet

File Name kbengine/http.c
Method static CURLcode header_append(struct Curl_easy *data,

```
....  
3038.          newbuff = realloc(data->state.headerbuff, newsize);
```

Wrong Size t Allocation\Path 13:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=506 |
| Status | New |

The function `reallocated_length` in `kbengine/schannel.c` at line 823 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | <code>kbengine/schannel.c</code> | <code>kbengine/schannel.c</code> |
| Line | 881 | 881 |
| Object | <code>reallocated_length</code> | <code>reallocated_length</code> |

Code Snippet

File Name `kbengine/schannel.c`
Method `schannel_connect_step2(struct connectdata *conn, int sockindex)`

```
....  
881.          reallocated_length);
```

Wrong Size t Allocation\Path 14:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=507 |
| Status | New |

The function `reallocated_length` in `kbengine/schannel.c` at line 1476 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | <code>kbengine/schannel.c</code> | <code>kbengine/schannel.c</code> |
| Line | 1538 | 1538 |
| Object | <code>reallocated_length</code> | <code>reallocated_length</code> |

Code Snippet

File Name `kbengine/schannel.c`
Method `schannel_recv(struct connectdata *conn, int sockindex,`

```
.....
1538.                                     reallocated_length);
```

Wrong Size t Allocation\Path 15:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=508 |
| Status | New |

The function `reallocated_length` in `kbengine/schannel.c` at line 1476 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | <code>kbengine/schannel.c</code> | <code>kbengine/schannel.c</code> |
| Line | 1624 | 1624 |
| Object | <code>reallocated_length</code> | <code>reallocated_length</code> |

Code Snippet

File Name `kbengine/schannel.c`
 Method `schannel_recv(struct connectdata *conn, int sockindex,`

```
.....
1624.                                     reallocated_length);
```

Wrong Size t Allocation\Path 16:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=509 |
| Status | New |

The function `items` in `kbengine/ldap.c` at line 789 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|------------------------------|------------------------------|
| File | <code>kbengine/ldap.c</code> | <code>kbengine/ldap.c</code> |
| Line | 803 | 803 |
| Object | <code>items</code> | <code>items</code> |

Code Snippet

File Name `kbengine/ldap.c`
 Method `*/`

```
.....
803.
```

Wrong Size t Allocation\Path 17:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=510 |
| Status | New |

The function sslsize in kbengine/url.c at line 1782 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 1795 | 1795 |
| Object | sslsizes | sslsizes |

Code Snippet

File Name kbengine/url.c
Method static struct connectdata *allocate_conn(struct Curl_easy *data)

```
.....
1795.      char *ssl = calloc(4, sslsize);
```

Wrong Size t Allocation\Path 18:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=511 |
| Status | New |

The function pathlen in kbengine/cookie.c at line 426 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 723 | 723 |
| Object | pathlen | pathlen |

Code Snippet

File Name kbengine/cookie.c
Method Curl_cookie_add(struct Curl_easy *data,


```
.....
723.          co->path = malloc(pathlen + 1); /* one extra for the zero
byte */
```

Wrong Size t Allocation\Path 19:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=512 |
| Status | New |

The function matches in kbengine/cookie.c at line 1215 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1289 | 1289 |
| Object | matches | matches |

Code Snippet

File Name kbengine/cookie.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
.....
1289.          array = malloc(sizeof(struct Cookie *) * matches);
```

Wrong Size t Allocation\Path 20:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=513 |
| Status | New |

The function working_path_len in kbengine/curl_path.c at line 32 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 49 | 49 |
| Object | working_path_len | working_path_len |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....  
49.         real_path = malloc(working_path_len + 1);
```

Wrong Size t Allocation\Path 21:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=514 |
| Status | New |

The function `working_path_len` in `kbengine/curl_path.c` at line 32 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------------------------|-----------------------------------|
| File | <code>kbengine/curl_path.c</code> | <code>kbengine/curl_path.c</code> |
| Line | 79 | 79 |
| Object | <code>working_path_len</code> | <code>working_path_len</code> |

Code Snippet

File Name `kbengine/curl_path.c`
Method `CURLcode Curl_getworkingpath(struct connectdata *conn,`

```
....  
79.         real_path = malloc(working_path_len + 1);
```

Wrong Size t Allocation\Path 22:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=515 |
| Status | New |

The function `nread` in `kbengine/ftp.c` at line 2602 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------------------|-----------------------------|
| File | <code>kbengine/ftp.c</code> | <code>kbengine/ftp.c</code> |
| Line | 2786 | 2786 |
| Object | <code>nread</code> | <code>nread</code> |

Code Snippet

File Name `kbengine/ftp.c`
Method `static CURLcode ftp_statemach_act(struct connectdata *conn)`

```
.....  
2786.          dir = malloc(nread + 1);
```

Wrong Size t Allocation\Path 23:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=516 |
| Status | New |

The function nread in kbengine/ftp.c at line 2602 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 2879 | 2879 |
| Object | nread | nread |

Code Snippet

File Name kbengine/ftp.c
Method static CURLcode ftp_statemach_act(struct connectdata *conn)

```
.....  
2879.          os = malloc(nread + 1);
```

Wrong Size t Allocation\Path 24:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=517 |
| Status | New |

The function len in kbengine/http.c at line 212 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 249 | 249 |
| Object | len | len |

Code Snippet

File Name kbengine/http.c
Method char *Curl_copy_header_value(const char *header)

```
....  
249.     value = malloc(len + 1);
```

Wrong Size t Allocation\Path 25:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=518 |
| Status | New |

The function nheader in kbengine/http2.c at line 1746 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http2.c | kbengine/http2.c |
| Line | 1834 | 1834 |
| Object | nheader | nheader |

Code Snippet

File Name kbengine/http2.c
Method static ssize_t http2_send(struct connectdata *conn, int sockindex,

```
....  
1834.     nva = malloc(sizeof(nghhttp2_nv) * nheader);
```

Wrong Size t Allocation\Path 26:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=519 |
| Status | New |

The function ca_file_bufsize in kbengine/schannel_verify.c at line 80 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------------------|----------------------------|
| File | kbengine/schannel_verify.c | kbengine/schannel_verify.c |
| Line | 143 | 143 |
| Object | ca_file_bufsize | ca_file_bufsize |

Code Snippet

File Name kbengine/schannel_verify.c
Method static CURLcode add_certs_to_store(HCERTSTORE trust_store,

```
.....
143.     ca_file_buffer = (char *)malloc(ca_file_bufsize + 1);
```

Wrong Size t Allocation\Path 27:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=520 |
| Status | New |

The function len in kbengine/schannel_verify.c at line 285 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------------------|----------------------------|
| File | kbengine/schannel_verify.c | kbengine/schannel_verify.c |
| Line | 321 | 321 |
| Object | len | len |

Code Snippet

File Name kbengine/schannel_verify.c
Method static CURLcode verify_host(struct Curl_easy *data,

```
.....
321.     cert_hostname_buff = (LPTSTR)malloc(len * sizeof(TCHAR));
```

Wrong Size t Allocation\Path 28:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=521 |
| Status | New |

The function len in kbengine/tool_cb_hdr.c at line 185 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|------------------------|------------------------|
| File | kbengine/tool_cb_hdr.c | kbengine/tool_cb_hdr.c |
| Line | 193 | 193 |
| Object | len | len |

Code Snippet

File Name kbengine/tool_cb_hdr.c
Method static char *parse_filename(const char *ptr, size_t len)

```
....  
193.     copy = malloc(len + 1);
```

Wrong Size t Allocation\Path 29:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=522 |
| Status | New |

The function len in kbengine/tool_doswin.c at line 135 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|------------------------|------------------------|
| File | kbengine/tool_doswin.c | kbengine/tool_doswin.c |
| Line | 175 | 175 |
| Object | len | len |

Code Snippet

File Name kbengine/tool_doswin.c
Method SANITIZEcode sanitize_file_name(char **const sanitized, const char *file_name,

```
....  
175.     target = malloc(len + 1);
```

Wrong Size t Allocation\Path 30:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=523 |
| Status | New |

The function len in kbengine/tool_doswin.c at line 482 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|------------------------|------------------------|
| File | kbengine/tool_doswin.c | kbengine/tool_doswin.c |
| Line | 508 | 508 |
| Object | len | len |

Code Snippet

File Name kbengine/tool_doswin.c
Method SANITIZEcode rename_if_reserved_dos_device_name(char **const sanitized,

```
....  
508.      *sanitized = malloc(len + 1);
```

Wrong Size t Allocation\Path 31:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=524 |
| Status | New |

The function ulen in kbengine/url.c at line 3233 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 3278 | 3278 |
| Object | ulen | ulen |

Code Snippet

File Name kbengine/url.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....  
3278.      ubuf = malloc(ulen + 1);
```

Wrong Size t Allocation\Path 32:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=525 |
| Status | New |

The function plen in kbengine/url.c at line 3233 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 3285 | 3285 |
| Object | plen | plen |

Code Snippet

File Name kbengine/url.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....  
3285.         pbuf = malloc(plen + 1);
```

Wrong Size t Allocation\Path 33:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=526 |
| Status | New |

The function olen in kbengine/url.c at line 3233 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 3294 | 3294 |
| Object | olen | olen |

Code Snippet

File Name kbengine/url.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....  
3294.         obuf = malloc(olen + 1);
```

Wrong Size t Allocation\Path 34:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=527 |
| Status | New |

The function urlllen in kbengine/url.c at line 4005 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 4073 | 4073 |
| Object | urlllen | urlllen |

Code Snippet

File Name kbengine/url.c
Method static CURLcode create_conn(struct Curl_easy *data,


```
....  
4073.      data->state.pathbuffer = malloc(urllen + 2);
```

Wrong Size t Allocation\Path 35:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=528 |
| Status | New |

The function urllen in kbengine/url.c at line 4005 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 4080 | 4080 |
| Object | urllen | urllen |

Code Snippet

File Name kbengine/url.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....  
4080.      conn->host.rawalloc = malloc(urllen + 2);
```

Wrong Size t Allocation\Path 36:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=529 |
| Status | New |

The function size in kbengine/vtls.c at line 805 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |
| Line | 919 | 919 |
| Object | size | size |

Code Snippet

File Name kbengine/vtls.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
.....
919.      buf = malloc(size + 1);
```

Wrong Size t Allocation\Path 37:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=530 |
| Status | New |

The function `addrlen` in `kbengine/ftp.c` at line 928 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------------------|-----------------------------|
| File | <code>kbengine/ftp.c</code> | <code>kbengine/ftp.c</code> |
| Line | 981 | 981 |
| Object | <code>addrlen</code> | <code>addrlen</code> |

Code Snippet

File Name `kbengine/ftp.c`
Method `static CURLcode ftp_state_use_port(struct connectdata *conn,`

```
.....
981.      addr = calloc(addrlen + 1, 1);
```

Wrong Size t Allocation\Path 38:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=531 |
| Status | New |

The function `timestampen` in `kbengine/pop3.c` at line 607 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|------------------------------|------------------------------|
| File | <code>kbengine/pop3.c</code> | <code>kbengine/pop3.c</code> |
| Line | 636 | 636 |
| Object | <code>timestampen</code> | <code>timestampen</code> |

Code Snippet

File Name `kbengine/pop3.c`
Method `static CURLcode pop3_state_servergreet_resp(struct connectdata *conn,`

```
.....
636.                pop3c->apoptimestamp = (char *)calloc(1, timestamplen +
1);
```

Wrong Size t Allocation\Path 39:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=532 |
| Status | New |

The function len in kbengine/_ctypes_test.c at line 213 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 216 | 216 |
| Object | len | len |

Code Snippet

File Name kbengine/_ctypes_test.c
Method EXPORT(wchar_t *) my_wcsdup(wchar_t *src)

```
.....
216.                wchar_t *ptr = (wchar_t *)malloc((len + 1) * sizeof(wchar_t));
```

Wrong Size t Allocation\Path 40:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=533 |
| Status | New |

The function homelen in kbengine/curl_path.c at line 32 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 63 | 63 |
| Object | homelen | homelen |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....  
63.         real_path = malloc(homelen + working_path_len + 1);
```

Wrong Size t Allocation\Path 41:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=534 |
| Status | New |

The function `working_path_len` in `kbengine/curl_path.c` at line 32 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 63 | 63 |
| Object | working_path_len | working_path_len |

Code Snippet

File Name kbengine/curl_path.c
Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....  
63.         real_path = malloc(homelen + working_path_len + 1);
```

Wrong Size t Allocation\Path 42:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=535 |
| Status | New |

The function `len` in `kbengine/dict.c` at line 94 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/dict.c | kbengine/dict.c |
| Line | 104 | 104 |
| Object | len | len |

Code Snippet

File Name kbengine/dict.c
Method static char *unescape_word(struct Curl_easy *data, const char *inputbuff)

```
....  
104.      dictp = malloc(len*2 + 1); /* add one for terminating zero */
```

Wrong Size t Allocation\Path 43:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=536 |
| Status | New |

The function currlen in kbengine/http.c at line 1867 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 2233 | 2233 |
| Object | currlen | currlen |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http(struct connectdata *conn, bool *done)

```
....  
2233.      newurl = malloc(urllen + newlen - currlen + 1);
```

Wrong Size t Allocation\Path 44:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=537 |
| Status | New |

The function newlen in kbengine/imap.c at line 1768 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1813 | 1813 |
| Object | newlen | newlen |

Code Snippet

File Name kbengine/imap.c
Method static char *imap_atom(const char *str, bool escape_only)

```
....  
1813.      newstr = (char *) malloc((newlen + 1) * sizeof(char));
```

Wrong Size t Allocation\Path 45:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=538 |
| Status | New |

The function prefixlen in kbengine/url.c at line 1985 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 2317 | 2317 |
| Object | prefixlen | prefixlen |

Code Snippet

File Name kbengine/url.c
Method static CURLcode parseurlandfillconn(struct Curl_easy *data,

```
....  
2317.      reurl = malloc(prefixlen + plen + 1);
```

Wrong Size t Allocation\Path 46:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=539 |
| Status | New |

The function plen in kbengine/url.c at line 1985 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 2317 | 2317 |
| Object | plen | plen |

Code Snippet

File Name kbengine/url.c
Method static CURLcode parseurlandfillconn(struct Curl_easy *data,

```
....  
2317.      reurl = malloc(prefixlen + plen + 1);
```

Wrong Size t Allocation\Path 47:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=540 |
| Status | New |

The function pem_len in kbengine/vtls.c at line 747 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |
| Line | 777 | 777 |
| Object | pem_len | pem_len |

Code Snippet

File Name kbengine/vtls.c
Method static CURLcode pubkey_pem_to_der(const char *pem,

```
....  
777.      stripped_pem = malloc(pem_len - pem_count + 1);
```

Wrong Size t Allocation\Path 48:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=541 |
| Status | New |

The function pem_count in kbengine/vtls.c at line 747 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |
| Line | 777 | 777 |
| Object | pem_count | pem_count |

Code Snippet

File Name kbengine/vtls.c
Method static CURLcode pubkey_pem_to_der(const char *pem,

```
....
777.     stripped_pem = malloc(pem_len - pem_count + 1);
```

Wrong Size t Allocation\Path 49:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=542 |
| Status | New |

The function newlen in kbengine/sds.c at line 129 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 142 | 142 |
| Object | newlen | newlen |

Code Snippet

File Name kbengine/sds.c
Method sds sdsMakeRoomFor(sds s, size_t addlen) {

```
....
142.     newsh = realloc(sh, sizeof *newsh+newlen+1);
```

Wrong Size t Allocation\Path 50:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=543 |
| Status | New |

The function urlllen in kbengine/http.c at line 1867 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 2233 | 2233 |
| Object | urlllen | urlllen |

Code Snippet

File Name kbengine/http.c
Method CURLcode Curl_http(struct connectdata *conn, bool *done)


```
.....
2233.          newurl = malloc(urllen + newlen - currlen + 1);
```

Integer Overflow

Query Path:

CPP\Cx\CPP Integer Overflow\Integer Overflow Version:0

Categories

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

FISMA 2014: System And Information Integrity

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Integer Overflow\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=550 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 186 of kbengine/a_int.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/a_int.c | kbengine/a_int.c |
| Line | 225 | 225 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/a_int.c
 Method ASN1_INTEGER *c2i_ASN1_INTEGER(ASN1_INTEGER **a, const unsigned char **pp,

```
.....
225.          i = len;
```

Integer Overflow\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=551 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 268 of kbengine/a_object.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|------|---------------------|---------------------|
| File | kbengine/a_object.c | kbengine/a_object.c |

| | | |
|--------|------------|------------|
| Line | 287 | 287 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/a_object.c

Method ASN1_OBJECT *c2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
287.         length = (int)len;
```

Integer Overflow\Path 3:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=552>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1354 of kbengine/e_aes.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 1418 | 1418 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes.c

Method static int aes_gcm_tls_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
1418.         rv = len + EVP_GCM_TLS_EXPLICIT_IV_LEN +
EVP_GCM_TLS_TAG_LEN;
```

Integer Overflow\Path 4:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=553>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1354 of kbengine/e_aes.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 1463 | 1463 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes.c

Method static int aes_gcm_tls_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....  
1463.          rv = len;
```

Integer Overflow\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=554>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1853 of kbengine/e_aes.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 1900 | 1900 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes.c

Method static int aes_ccm_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....  
1900.          rv = len;
```

Integer Overflow\Path 6:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=555>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 207 of kbengine/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 235 | 235 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
235.         frag = (unsigned int)inp_len >> (1 + n4x);
```

Integer Overflow\Path 7:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=556 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 207 of kbengine/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 236 | 236 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....  
236.         last = (unsigned int)inp_len + frag - (frag << (1 + n4x));
```

Integer Overflow\Path 8:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=557 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 455 of kbengine/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 517 | 517 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
.....
517.                for (l = len - plen - 1; plen < len; plen++)
```

Integer Overflow\Path 9:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=558 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 455 of kbengine/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 577 | 577 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
.....
577.                maxpad = len - (SHA_DIGEST_LENGTH + 1);
```

Integer Overflow\Path 10:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=559 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 455 of kbengine/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 628 | 628 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
628.                bitlen = key->md.Nl + (inp_len << 3); /* at most 18
bits */
```

Integer Overflow\Path 11:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=560 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 455 of kbengine/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 584 | 584 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
584.                ret &= (int)mask;
```

Integer Overflow\Path 12:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=561 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 455 of kbengine/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 746 | 746 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....  
746.                                cmask =
```

Integer Overflow\Path 13:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=562 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 455 of kbengine/e_aes_cbc_hmac_sha1.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 750 | 750 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....  
750.                                cmask &= ((int)(off - 1 - j)) >> (sizeof(int)  
* 8 - 1);
```

Integer Overflow\Path 14:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=563 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 203 of kbengine/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 232 | 232 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
232.         frag = (unsigned int)inp_len >> (1 + n4x);
```

Integer Overflow\Path 15:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=564 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 203 of kbengine/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 233 | 233 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c
Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
....
233.         last = (unsigned int)inp_len + frag - (frag << (1 + n4x));
```

Integer Overflow\Path 16:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=565 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 470 of kbengine/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 545 | 545 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,


```
.....
545.                for (l = len - plen - 1; plen < len; plen++)
```

Integer Overflow\Path 17:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=566 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 470 of kbengine/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 588 | 588 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
.....
588.                maxpad = len - (SHA256_DIGEST_LENGTH + 1);
```

Integer Overflow\Path 18:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=567 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 470 of kbengine/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 616 | 616 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
.....
616.                bitlen = key->md.Nl + (inp_len << 3); /* at most 18
bits */
```

Integer Overflow\Path 19:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=568 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 470 of kbengine/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 595 | 595 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
.....
595.                ret &= (int)mask;
```

Integer Overflow\Path 20:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=569 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 470 of kbengine/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 750 | 750 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
.....  
750.                                cmask =
```

Integer Overflow\Path 21:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=570 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 470 of kbengine/e_aes_cbc_hmac_sha256.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 754 | 754 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c
Method static int aesni_cbc_hmac_sha256_cipher(EVP_CIPHER_CTX *ctx,

```
.....  
754.                                cmask &= ((int)(off - 1 - j)) >> (sizeof(int)  
* 8 - 1);
```

Integer Overflow\Path 22:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=571 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 115 of kbengine/e_rc4_hmac_md5.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/e_rc4_hmac_md5.c | kbengine/e_rc4_hmac_md5.c |
| Line | 193 | 193 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/e_rc4_hmac_md5.c
Method static int rc4_hmac_md5_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....  
193.          l = (key->md.Nl + (blocks << 3)) & 0xffffffffU;
```

Integer Overflow\Path 23:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=572 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 988 of kbengine/multi.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 1017 | 1017 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/multi.c
Method CURLMcode curl_multi_wait(struct Curl_multi *multi,

```
....  
1017.          timeout_ms = (int)timeout_internal;
```

Integer Overflow\Path 24:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=573 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 485 of kbengine/obj_dat.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/obj_dat.c | kbengine/obj_dat.c |
| Line | 558 | 558 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/obj_dat.c
Method int OBJ_obj2txt(char *buf, int buf_len, const ASN1_OBJECT *a, int no_name)

```
....  
558.          i = (int)(l / 40);
```

Integer Overflow\Path 25:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=574 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 334 of kbengine/s2_clnt.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s2_clnt.c | kbengine/s2_clnt.c |
| Line | 391 | 391 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s2_clnt.c
Method static int get_server_hello(SSL *s)

```
....  
391.         j = (int)len - s->init_num;
```

Integer Overflow\Path 26:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=575 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 373 of kbengine/s2_srvr.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s2_srvr.c | kbengine/s2_srvr.c |
| Line | 443 | 443 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s2_srvr.c
Method static int get_client_master_key(SSL *s)

```
....  
443.         n = (int)len - s->init_num;
```

Integer Overflow\Path 27:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=576 |

[33&pathid=576](#)

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 560 of kbengine/s2_srvr.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s2_srvr.c | kbengine/s2_srvr.c |
| Line | 623 | 623 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s2_srvr.c

Method static int get_client_hello(SSL *s)

```
....  
623.      n = (int)len - s->init_num;
```

Integer Overflow\Path 28:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=577>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 833 of kbengine/s2_srvr.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s2_srvr.c | kbengine/s2_srvr.c |
| Line | 869 | 869 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s2_srvr.c

Method static int get_client_finished(SSL *s)

```
....  
869.      n = (int)len - s->init_num;
```

Integer Overflow\Path 29:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=578>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 934 of kbengine/s2_srvr.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s2_srvr.c | kbengine/s2_srvr.c |
| Line | 1047 | 1047 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s2_srvr.c

Method static int request_certificate(SSL *s)

```
....  
1047.         j = (int)len - s->init_num;
```

Integer Overflow\Path 30:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=579>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 297 of kbengine/s23_clnt.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/s23_clnt.c | kbengine/s23_clnt.c |
| Line | 313 | 313 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s23_clnt.c

Method static int ssl23_client_hello(SSL *s)

```
....  
313.         ssl2_compat = (options & SSL_OP_NO_SSLv2) ? 0 : 1;
```

Integer Overflow\Path 31:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=580>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2449 of kbengine/s3_clnt.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|------|--------------------|--------------------|
| File | kbengine/s3_clnt.c | kbengine/s3_clnt.c |

| | | |
|--------|------------|------------|
| Line | 3045 | 3045 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s3_clnt.c
Method int ssl3_send_client_key_exchange(SSL *s)

```
....
3045.                n = msglen + 3;
```

Integer Overflow\Path 32:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=581 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2449 of kbengine/s3_clnt.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_clnt.c | kbengine/s3_clnt.c |
| Line | 3048 | 3048 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s3_clnt.c
Method int ssl3_send_client_key_exchange(SSL *s)

```
....
3048.                n = msglen + 2;
```

Integer Overflow\Path 33:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=582 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2449 of kbengine/s3_clnt.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_clnt.c | kbengine/s3_clnt.c |
| Line | 3178 | 3178 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s3_clnt.c

Method int ssl3_send_client_key_exchange(SSL *s)

```
....  
3178.                n = 2 + identity_len;
```

Integer Overflow\Path 34:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=583>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 497 of kbengine/s3_enc.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_enc.c | kbengine/s3_enc.c |
| Line | 531 | 531 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s3_enc.c

Method int ssl3_enc(SSL *s, int send)

```
....  
531.                i = bs - ((int)1 % bs);
```

Integer Overflow\Path 35:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=584>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 721 of kbengine/s3_enc.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_enc.c | kbengine/s3_enc.c |
| Line | 748 | 748 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s3_enc.c

Method int n_ssl3_mac(SSL *ssl, unsigned char *md, int send)

```
.....  
748.         npad = (48 / md_size) * md_size;
```

Integer Overflow\Path 36:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=585 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2131 of kbengine/s3_srvr.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_srvr.c | kbengine/s3_srvr.c |
| Line | 2334 | 2334 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s3_srvr.c
Method int ssl3_get_client_key_exchange(SSL *s)

```
.....  
2334.         i = (int)n;
```

Integer Overflow\Path 37:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=586 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 425 of kbengine/sds.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 434 | 434 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/sds.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
.....  
434.         i = initlen; /* Position of the next byte to write to dest  
str. */
```

Integer Overflow\Path 38:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=587 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 575 of kbengine/sds.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 581 | 581 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/sds.c
Method void sdsrange(sds s, int start, int end) {

```
....  
581.         start = len+start;
```

Integer Overflow\Path 39:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=588 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 575 of kbengine/sds.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 585 | 585 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/sds.c
Method void sdsrange(sds s, int start, int end) {

```
....  
585.         end = len+end;
```

Integer Overflow\Path 40:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=589 |

| | |
|--------|--|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=589 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 575 of kbengine/sds.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 593 | 593 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/sds.c

Method void sdsrange(sds s, int start, int end) {

```
....  
593.             end = len-1;
```

Integer Overflow\Path 41:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=590>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 152 of kbengine/t1_enc.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/t1_enc.c | kbengine/t1_enc.c |
| Line | 219 | 219 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/t1_enc.c

Method static int t1s1_P_hash(const EVP_MD *md, const unsigned char *sec,

```
....  
219.             olen -= j;
```

Integer Overflow\Path 42:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=591>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 751 of kbengine/t1_enc.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/t1_enc.c | kbengine/t1_enc.c |
| Line | 859 | 859 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/t1_enc.c
Method int tls1_enc(SSL *s, int send)

```
....
859.                for (k = (int)l; k < (int)(l + i); k++)
```

Integer Overflow\Path 43:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=592 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 751 of kbengine/t1_enc.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/t1_enc.c | kbengine/t1_enc.c |
| Line | 854 | 854 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/t1_enc.c
Method int tls1_enc(SSL *s, int send)

```
....
854.                j = i - 1;
```

Integer Overflow\Path 44:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=593 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3572 of kbengine/url.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

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

| | | |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 3650 | 3650 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/url.c

Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....  
3650.          port = (int)portparse; /* we know it will fit */
```

Integer Overflow\Path 45:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=594>

Status New

A variable of a larger data type, memlen, is being assigned to a smaller data type, in 690 of kbengine/cyassl.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cyassl.c | kbengine/cyassl.c |
| Line | 698 | 698 |
| Object | memlen | memlen |

Code Snippet

File Name kbengine/cyassl.c

Method static ssize_t cyassl_send(struct connectdata *conn,

```
....  
698.    int  memlen = (len > (size_t)INT_MAX) ? INT_MAX : (int)len;
```

Integer Overflow\Path 46:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=595>

Status New

A variable of a larger data type, buffsize, is being assigned to a smaller data type, in 736 of kbengine/cyassl.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cyassl.c | kbengine/cyassl.c |
| Line | 744 | 744 |
| Object | buffsize | buffsize |

Code Snippet

File Name kbengine/cyassl.c

Method static ssize_t cyassl_recv(struct connectdata *conn,

```
....
744.     int  buffsize = (buffersize > (size_t)INT_MAX) ? INT_MAX :
(int)buffersize;
```

Integer Overflow\Path 47:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=596>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 169 of kbengine/b_print.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/b_print.c | kbengine/b_print.c |
| Line | 186 | 186 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/b_print.c

Method _dopr(char **sbuffer,

```
....
186.     flags = currlen = cflags = min = 0;
```

Long Overflow

Query Path:

CPP\Cx\CPP Integer Overflow\Long Overflow Version:0

Categories

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

FISMA 2014: System And Information Integrity

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Long Overflow\Path 1:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=597>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 491 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 491 | 491 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c
Method EXPORT(double) tf_d(double c) { S; return c/3; }

```
....  
491.  EXPORT(double) tf_d(double c) { S; return c/3; }
```

Long Overflow\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=598 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 492 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 492 | 492 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c
Method EXPORT(long double) tf_D(long double c) { S; return c/3; }

```
....  
492.  EXPORT(long double) tf_D(long double c) { S; return c/3; }
```

Long Overflow\Path 3:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=599 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 506 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 506 | 506 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c

Method EXPORT(double) __stdcall s_tf_d(double c) { S; return c/3; }

```
....
506.  EXPORT(double) __stdcall s_tf_d(double c) { S; return c/3; }
```

Long Overflow\Path 4:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=600>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 507 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 507 | 507 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c

Method EXPORT(long double) __stdcall s_tf_D(long double c) { S; return c/3; }

```
....
507.  EXPORT(long double) __stdcall s_tf_D(long double c) { S; return
c/3; }
```

Long Overflow\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=601>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 522 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

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

| | | |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 522 | 522 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c

Method EXPORT(double) tf_bd(signed char x, double c) { S; return c/3; }

```
....
522.  EXPORT(double) tf_bd(signed char x, double c) { S; return c/3; }
```

Long Overflow\Path 6:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=602>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 523 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 523 | 523 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c

Method EXPORT(long double) tf_bd(signed char x, long double c) { S; return c/3; }

```
....
523.  EXPORT(long double) tf_bd(signed char x, long double c) { S;
return c/3; }
```

Long Overflow\Path 7:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=603>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 538 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |

| | | |
|--------|------------|------------|
| Line | 538 | 538 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c

Method EXPORT(double) __stdcall s_tf_bd(signed char x, double c) { S; return c/3; }

```
....
538.  EXPORT(double) __stdcall s_tf_bd(signed char x, double c) { S;
return c/3; }
```

Long Overflow\Path 8:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=604>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 539 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 539 | 539 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c

Method EXPORT(long double) __stdcall s_tf_bD(signed char x, long double c) { S; return c/3; }

```
....
539.  EXPORT(long double) __stdcall s_tf_bD(signed char x, long double
c) { S; return c/3; }
```

Long Overflow\Path 9:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=605>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 571 of kbengine/b_print.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|------|--------------------|--------------------|
| File | kbengine/b_print.c | kbengine/b_print.c |

| | | |
|--------|------------|------------|
| Line | 574 | 574 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/b_print.c

Method static long roundv(LDOUBLE value)

```
....
574.      intpart = (long)value;
```

Long Overflow\Path 10:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=606>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 582 of kbengine/b_print.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/b_print.c | kbengine/b_print.c |
| Line | 609 | 609 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/b_print.c

Method fmtfp(char **sbuffer,

```
....
609.      intpart = (long)ufvalue;
```

Long Overflow\Path 11:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=607>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 490 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 490 | 490 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c
Method EXPORT(float) tf_f(float c) { S; return c/3; }

```
....  
490.  EXPORT(float) tf_f(float c) { S; return c/3; }
```

Long Overflow\Path 12:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=608>
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 505 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 505 | 505 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c
Method EXPORT(float) __stdcall s_tf_f(float c) { S; return c/3; }

```
....  
505.  EXPORT(float) __stdcall s_tf_f(float c) { S; return c/3; }
```

Long Overflow\Path 13:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=609>
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 521 of kbengine/_ctypes_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 521 | 521 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctypes_test.c

Method EXPORT(float) tf_bf(signed char x, float c) { S; return c/3; }

```
....
521.  EXPORT(float) tf_bf(signed char x, float c) { S; return c/3; }
```

Long Overflow\Path 14:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=610 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 537 of kbengine/_ctype_test.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|------------------------|------------------------|
| File | kbengine/_ctype_test.c | kbengine/_ctype_test.c |
| Line | 537 | 537 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/_ctype_test.c
Method EXPORT(float) __stdcall s_tf_bf(signed char x, float c) { S; return c/3; }

```
....
537.  EXPORT(float) __stdcall s_tf_bf(signed char x, float c) { S;
return c/3; }
```

Use of Uninitialized Pointer

Query Path:

CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Pointer\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1283 |
| Status | New |

The variable declared in strtup at kbengine/tasn_enc.c in line 541 is not initialized when it is used by flags at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |

| | | |
|--------|--------|-------|
| Line | 545 | 644 |
| Object | strtmp | flags |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
545.     ASN1_STRING *strtmp;
....
644.     && (strtmp->flags & ASN1_STRING_FLAG_NDEF)) {
```

Use of Uninitialized Pointer\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1284>

Status New

The variable declared in strtmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by type at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 545 | 566 |
| Object | strtmp | type |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
545.     ASN1_STRING *strtmp;
....
566.     utype = strtmp->type;
```

Use of Uninitialized Pointer\Path 3:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1285>

Status New

The variable declared in strtmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by data at kbengine/tasn_enc.c in line 541.

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

| | | |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 545 | 646 |
| Object | strtmp | data |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
545.     ASN1_STRING *strtmp;
....
646.           strtmp->data = cout;
```

Use of Uninitialized Pointer\Path 4:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1286>

Status New

The variable declared in strtmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by length at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 545 | 647 |
| Object | strtmp | length |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
545.     ASN1_STRING *strtmp;
....
647.           strtmp->length = 0;
```

Use of Uninitialized Pointer\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1287>

Status New

The variable declared in strtmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by data at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 545 | 652 |
| Object | strtmp | data |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```

....
545.     ASN1_STRING *strtmp;
....
652.         cont = strtmp->data;

```

Use of Uninitialized Pointer\Path 6:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1288>

Status New

The variable declared in strtmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by length at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 545 | 653 |
| Object | strtmp | length |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```

....
545.     ASN1_STRING *strtmp;
....
653.         len = strtmp->length;

```

Use of Uninitialized Pointer\Path 7:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1289>

Status New

The variable declared in strtmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by flags at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 545 | 644 |
| Object | strtmp | flags |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```

....
545.     ASN1_STRING *strtmp;
....
644.         && (strtmp->flags & ASN1_STRING_FLAG_NDEF)) {

```

Use of Uninitialized Pointer\Path 8:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1290>

Status New

The variable declared in strtmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by data at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 545 | 646 |
| Object | strtmp | data |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```

....
545.     ASN1_STRING *strtmp;
....
646.         strtmp->data = cout;

```

Use of Uninitialized Pointer\Path 9:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1291>

Status New

The variable declared in strtmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by length at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 545 | 647 |
| Object | strtmp | length |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
545.     ASN1_STRING *strtmp;
....
647.             strtmp->length = 0;
```

Use of Uninitialized Pointer\Path 10:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1292>

Status New

The variable declared in strtmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by data at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 545 | 652 |
| Object | strtmp | data |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
545.     ASN1_STRING *strtmp;
....
652.     cont = strtmp->data;
```

Use of Uninitialized Pointer\Path 11:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1293>

Status New

The variable declared in strtmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by length at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 545 | 653 |
| Object | strtmp | length |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
.....
545.     ASN1_STRING *strtmp;
.....
653.         len = strtmp->length;
```

Use of Uninitialized Pointer\Path 12:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1294>

Status New

The variable declared in otmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by otmp at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 546 | 582 |
| Object | otmp | otmp |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
.....
546.     ASN1_OBJECT *otmp;
.....
582.         len = otmp->length;
```

Use of Uninitialized Pointer\Path 13:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1295>

Status New

The variable declared in otmp at kbengine/tasn_enc.c in line 541 is not initialized when it is used by data at kbengine/tasn_enc.c in line 541.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 546 | 581 |
| Object | otmp | data |

Code Snippet

File Name kbengine/tasn_enc.c

Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....  
546.     ASN1_OBJECT *otmp;  
....  
581.     cont = otmp->data;
```

Divide By Zero

Query Path:

CPP\Cx\CPP Medium Threat\Divide By Zero Version:1

[Description](#)

Divide By Zero\Path 1:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=406>

Status New

The application performs an illegal operation in `tls_fips_digest_extra`, in `kbengine/s3_cbc.c`. In line 781, the program attempts to divide by `block_size`, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input `block_size` in `tls_fips_digest_extra` of `kbengine/s3_cbc.c`, at line 781.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_cbc.c | kbengine/s3_cbc.c |
| Line | 809 | 809 |
| Object | block_size | block_size |

Code Snippet

File Name kbengine/s3_cbc.c

Method void tls_fips_digest_extra(const EVP_CIPHER_CTX *cipher_ctx,

```
....  
809.     blocks_orig = (orig_len + digest_pad) / block_size;
```

Divide By Zero\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=407>

Status New

The application performs an illegal operation in `tls_fips_digest_extra`, in `kbengine/s3_cbc.c`. In line 781, the program attempts to divide by `block_size`, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input `block_size` in `tls_fips_digest_extra` of `kbengine/s3_cbc.c`, at line 781.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_cbc.c | kbengine/s3_cbc.c |
| Line | 810 | 810 |
| Object | block_size | block_size |

Code Snippet

File Name kbengine/s3_cbc.c

Method void tls_fips_digest_extra(const EVP_CIPHER_CTX *cipher_ctx,

```
....  
810.         blocks_data = (data_len + digest_pad) / block_size;
```

Divide By Zero\Path 3:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=408>

Status New

The application performs an illegal operation in `ssl3_enc`, in `kbengine/s3_enc.c`. In line 497, the program attempts to divide by `bs`, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input `bs` in `ssl3_enc` of `kbengine/s3_enc.c`, at line 497.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_enc.c | kbengine/s3_enc.c |
| Line | 531 | 531 |
| Object | bs | bs |

Code Snippet

File Name kbengine/s3_enc.c

Method int ssl3_enc(SSL *s, int send)

```
....  
531.         i = bs - ((int)1 % bs);
```

Divide By Zero\Path 4:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=409>

Status New

The application performs an illegal operation in ssl3_enc, in kbengine/s3_enc.c. In line 497, the program attempts to divide by bs, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input bs in ssl3_enc of kbengine/s3_enc.c, at line 497.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_enc.c | kbengine/s3_enc.c |
| Line | 545 | 545 |
| Object | bs | bs |

Code Snippet

File Name kbengine/s3_enc.c

Method int ssl3_enc(SSL *s, int send)

```
....  
545.          if (1 == 0 || 1 % bs != 0)
```

Divide By Zero\Path 5:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=410>

Status New

The application performs an illegal operation in ssl3_handshake_mac, in kbengine/s3_enc.c. In line 665, the program attempts to divide by n, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input n in ssl3_handshake_mac of kbengine/s3_enc.c, at line 665.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_enc.c | kbengine/s3_enc.c |
| Line | 699 | 699 |
| Object | n | n |

Code Snippet

File Name kbengine/s3_enc.c

Method static int ssl3_handshake_mac(SSL *s, int md_nid,

```
....  
699.          npad = (48 / n) * n;
```

Divide By Zero\Path 6:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=411>

Status New

The application performs an illegal operation in `n_ssl3_mac`, in `kbengine/s3_enc.c`. In line 721, the program attempts to divide by `md_size`, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input `md_size` in `n_ssl3_mac` of `kbengine/s3_enc.c`, at line 721.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_enc.c | kbengine/s3_enc.c |
| Line | 748 | 748 |
| Object | md_size | md_size |

Code Snippet

File Name kbengine/s3_enc.c

Method `int n_ssl3_mac(SSL *ssl, unsigned char *md, int send)`

```
....  
748.      npad = (48 / md_size) * md_size;
```

Divide By Zero\Path 7:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=412>

Status New

The application performs an illegal operation in `tls1_PRF`, in `kbengine/t1_enc.c`. In line 242, the program attempts to divide by `count`, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input `count` in `tls1_PRF` of `kbengine/t1_enc.c`, at line 242.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/t1_enc.c | kbengine/t1_enc.c |
| Line | 268 | 268 |
| Object | count | count |

Code Snippet

File Name kbengine/t1_enc.c

Method `static int tls1_PRF(long digest_mask,`

```
....  
268.      len = slen / count;
```

Divide By Zero\Path 8:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=412>

[33&pathid=413](#)

Status New

The application performs an illegal operation in `tls1_enc`, in `kbengine/t1_enc.c`. In line 751, the program attempts to divide by `bs`, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input `bs` in `tls1_enc` of `kbengine/t1_enc.c`, at line 751.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | <code>kbengine/t1_enc.c</code> | <code>kbengine/t1_enc.c</code> |
| Line | 849 | 849 |
| Object | <code>bs</code> | <code>bs</code> |

Code Snippet

File Name `kbengine/t1_enc.c`

Method `int tls1_enc(SSL *s, int send)`

```
....
849.         i = bs - ((int)l % bs);
```

Divide By Zero\Path 9:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=414>

Status New

The application performs an illegal operation in `seedArrayWithPolyCenter`, in `kbengine/RecastMeshDetail.cpp`. In line 883, the program attempts to divide by `npoly`, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input `npoly` in `seedArrayWithPolyCenter` of `kbengine/RecastMeshDetail.cpp`, at line 883.

| | Source | Destination |
|--------|--|--|
| File | <code>kbengine/RecastMeshDetail.cpp</code> | <code>kbengine/RecastMeshDetail.cpp</code> |
| Line | 934 | 934 |
| Object | <code>npoly</code> | <code>npoly</code> |

Code Snippet

File Name `kbengine/RecastMeshDetail.cpp`

Method `static void seedArrayWithPolyCenter(rcContext* ctx, const rcCompactHeightfield& chf,`

```
....
934.         pcx /= npoly;
```

Divide By Zero\Path 10:

Severity Medium

Result State To Verify

Online Results [http://WIN-](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=414)

BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=415

Status New

The application performs an illegal operation in seedArrayWithPolyCenter, in kbengine/RecastMeshDetail.cpp. In line 883, the program attempts to divide by npoly, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input npoly in seedArrayWithPolyCenter of kbengine/RecastMeshDetail.cpp, at line 883.

| | Source | Destination |
|--------|-------------------------------|-------------------------------|
| File | kbengine/RecastMeshDetail.cpp | kbengine/RecastMeshDetail.cpp |
| Line | 935 | 935 |
| Object | npoly | npoly |

Code Snippet

File Name kbengine/RecastMeshDetail.cpp

Method static void seedArrayWithPolyCenter(rcContext* ctx, const rcCompactHeightfield& chf,

```
....
935.         pcy /= npoly;
```

Divide By Zero\Path 11:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=416>

Status New

The application performs an illegal operation in polyMinExtent, in kbengine/RecastMeshDetail.cpp. In line 536, the program attempts to divide by nverts, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input nverts in polyMinExtent of kbengine/RecastMeshDetail.cpp, at line 536.

| | Source | Destination |
|--------|-------------------------------|-------------------------------|
| File | kbengine/RecastMeshDetail.cpp | kbengine/RecastMeshDetail.cpp |
| Line | 541 | 541 |
| Object | nverts | nverts |

Code Snippet

File Name kbengine/RecastMeshDetail.cpp

Method static float polyMinExtent(const float* verts, const int nverts)

```
....
541.         const int ni = (i+1) % nverts;
```

Heap Inspection

Query Path:

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
 FISMA 2014: Media Protection
 NIST SP 800-53: SC-4 Information in Shared Resources (P1)
 OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Heap Inspection\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1173 |
| Status | New |

Method http_output_basic at line 265 of kbengine/http.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 272 | 272 |
| Object | pwd | pwd |

Code Snippet

File Name kbengine/http.c
 Method static CURLcode http_output_basic(struct connectdata *conn, bool proxy)

```
....
272.     const char *pwd;
```

Heap Inspection\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1174 |
| Status | New |

Method rtsp_do at line 248 of kbengine/rtsp.c defines p_proxyuserpwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to p_proxyuserpwd, this variable is never cleared from memory.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/rtsp.c | kbengine/rtsp.c |
| Line | 268 | 268 |
| Object | p_proxyuserpwd | p_proxyuserpwd |

Code Snippet

File Name kbengine/rtsp.c

Method static CURLcode rtsp_do(struct connectdata *conn, bool *done)

```
....  
268.     const char *p_proxyuserpwd = NULL;
```

Heap Inspection\Path 3:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1175 |
| Status | New |

Method rtsp_do at line 248 of kbengine/rtsp.c defines p_userpwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to p_userpwd, this variable is never cleared from memory.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/rtsp.c | kbengine/rtsp.c |
| Line | 269 | 269 |
| Object | p_userpwd | p_userpwd |

Code Snippet

File Name kbengine/rtsp.c
Method static CURLcode rtsp_do(struct connectdata *conn, bool *done)

```
....  
269.     const char *p_userpwd = NULL;
```

Heap Inspection\Path 4:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1176 |
| Status | New |

Method SRP_VBASE_init at line 358 of kbengine/srp_vfy.c defines user_pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to user_pwd, this variable is never cleared from memory.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/srp_vfy.c | kbengine/srp_vfy.c |
| Line | 367 | 367 |
| Object | user_pwd | user_pwd |

Code Snippet

File Name kbengine/srp_vfy.c
Method int SRP_VBASE_init(SRP_VBASE *vb, char *verifier_file)

```
....
367.      SRP_user_pwd *user_pwd = NULL;
```

Heap Inspection\Path 5:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1177 |
| Status | New |

Method gskit_connect_step1 at line 795 of kbengine/gskit.c defines keyringpwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to keyringpwd, this variable is never cleared from memory.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 803 | 803 |
| Object | keyringpwd | keyringpwd |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```
....
803.      const char * const keyringpwd = SSL_SET_OPTION(key_passwd);
```

Heap Inspection\Path 6:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1178 |
| Status | New |

Method CMS_RecipientInfo_set0_password at line 66 of kbengine/cms_pwri.c defines passlen, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passlen, this variable is never cleared from memory.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/cms_pwri.c | kbengine/cms_pwri.c |
| Line | 67 | 67 |
| Object | passlen | passlen |

Code Snippet

File Name kbengine/cms_pwri.c
Method int CMS_RecipientInfo_set0_password(CMS_RecipientInfo *ri,

```
.....
67.                                unsigned char *pass,
ossl_ssize_t passlen)
```

Heap Inspection\Path 7:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1179 |
| Status | New |

Method `imap_perform_login` at line 490 of `kbengine/imap.c` defines `passwd`, which is designated to contain user passwords. However, while plaintext passwords are later assigned to `passwd`, this variable is never cleared from memory.

| | Source | Destination |
|--------|------------------------------|------------------------------|
| File | <code>kbengine/imap.c</code> | <code>kbengine/imap.c</code> |
| Line | 494 | 494 |
| Object | <code>passwd</code> | <code>passwd</code> |

Code Snippet

File Name `kbengine/imap.c`
Method `static CURLcode imap_perform_login(struct connectdata *conn)`

```
.....
494.    char *passwd;
```

Heap Inspection\Path 8:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1180 |
| Status | New |

Method at line 253 of `kbengine/ldap.c` defines `passwd`, which is designated to contain user passwords. However, while plaintext passwords are later assigned to `passwd`, this variable is never cleared from memory.

| | Source | Destination |
|--------|------------------------------|------------------------------|
| File | <code>kbengine/ldap.c</code> | <code>kbengine/ldap.c</code> |
| Line | 277 | 277 |
| Object | <code>passwd</code> | <code>passwd</code> |

Code Snippet

File Name `kbengine/ldap.c`
Method

```
....
277.      char *user = NULL;
```

Heap Inspection\Path 9:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1181 |
| Status | New |

Method create_conn at line 4005 of kbengine/url.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 4014 | 4014 |
| Object | passwd | passwd |

Code Snippet

File Name kbengine/url.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
4014.      char *passwd = NULL;
```

Buffer Overflow AddressOfLocalVarReturned

Query Path:

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow AddressOfLocalVarReturned\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=190 |
| Status | New |

The pointer aes_256_wrap at kbengine/e_aes.c in line 2021 is being used after it has been freed.

| | Source | Destination |
|------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 2023 | 2023 |

| | | |
|--------|--------------|--------------|
| Object | aes_256_wrap | aes_256_wrap |
|--------|--------------|--------------|

Code Snippet

File Name kbengine/e_aes.c
Method const EVP_CIPHER *EVP_aes_256_wrap(void)

```
....  
2023.      return &aes_256_wrap;
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=191 |
| Status | New |

The pointer aes_128_wrap at kbengine/e_aes.c in line 1993 is being used after it has been freed.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 1995 | 1995 |
| Object | aes_128_wrap | aes_128_wrap |

Code Snippet

File Name kbengine/e_aes.c
Method const EVP_CIPHER *EVP_aes_128_wrap(void)

```
....  
1995.      return &aes_128_wrap;
```

Buffer Overflow AddressOfLocalVarReturned\Path 3:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=192 |
| Status | New |

The pointer aes_192_wrap at kbengine/e_aes.c in line 2007 is being used after it has been freed.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 2009 | 2009 |
| Object | aes_192_wrap | aes_192_wrap |

Code Snippet

File Name kbengine/e_aes.c

Method const EVP_CIPHER *EVP_aes_192_wrap(void)

```
....  
2009.      return &aes_192_wrap;
```

Buffer Overflow AddressOfLocalVarReturned\Path 4:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=193 |
| Status | New |

The pointer d2 at kbengine/tasn_enc.c in line 407 is being used after it has been freed.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/tasn_enc.c | kbengine/tasn_enc.c |
| Line | 415 | 415 |
| Object | d2 | d2 |

Code Snippet

File Name kbengine/tasn_enc.c
Method static int der_cmp(const void *a, const void *b)

```
....  
415.      return d1->length - d2->length;
```

Buffer Overflow AddressOfLocalVarReturned\Path 5:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=194 |
| Status | New |

The pointer str at kbengine/http2.c in line 331 is being used after it has been freed.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http2.c | kbengine/http2.c |
| Line | 350 | 350 |
| Object | str | str |

Code Snippet

File Name kbengine/http2.c
Method const char *Curl_http2_strerror(uint32_t err)

```
....
350.      return (err < sizeof(str) / sizeof(str[0])) ? str[err] :
"unknown";
```

Short Overflow

Query Path:

CPP\Cx\CPP Integer Overflow\Short Overflow Version:1

Categories

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

FISMA 2014: System And Information Integrity

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Short Overflow\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=611 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 191 of kbengine/blast.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/blast.c | kbengine/blast.c |
| Line | 206 | 206 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/blast.c
Method local int construct(struct huffman *h, const unsigned char *rep, int n)

```
....
206.          length[symbol++] = len;
```

Short Overflow\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=612 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 572 of kbengine/d1_pkt.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|------|-------------------|-------------------|
| File | kbengine/d1_pkt.c | kbengine/d1_pkt.c |
| Line | 623 | 623 |

| | | |
|--------|------------|------------|
| Object | AssignExpr | AssignExpr |
|--------|------------|------------|

Code Snippet

File Name kbengine/d1_pkt.c
Method int dtls1_get_record(SSL *s)

```
....
623.          version = (ssl_major << 8) | ssl_minor;
```

Short Overflow\Path 3:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=613 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 665 of kbengine/puff.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/puff.c | kbengine/puff.c |
| Line | 711 | 711 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/puff.c
Method local int dynamic(struct state *s)

```
....
711.          lengths[index++] = symbol;
```

Short Overflow\Path 4:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=614 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 665 of kbengine/puff.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/puff.c | kbengine/puff.c |
| Line | 727 | 727 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/puff.c

Method local int dynamic(struct state *s)

```
....  
727. lengths[index++] = len;
```

Short Overflow\Path 5:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=615 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 306 of kbengine/s3_pkt.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_pkt.c | kbengine/s3_pkt.c |
| Line | 353 | 353 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/s3_pkt.c
Method static int ssl3_get_record(SSL *s)

```
....  
353. version = (ssl_major << 8) | ssl_minor;
```

Double Free

Query Path:

CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description

Double Free\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1164 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/ldap.c | kbengine/ldap.c |
| Line | 935 | 935 |
| Object | attributes | attributes |

Code Snippet

File Name kbengine/ldap.c
Method */

```
....  
935.         if(result) {
```

Double Free\Path 2:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1165>
Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/ldap.c | kbengine/ldap.c |
| Line | 950 | 950 |
| Object | attributes | attributes |

Code Snippet

File Name kbengine/ldap.c
Method */

```
....  
950.         if(!ludp->lud_attrs[i]) {
```

Double Free\Path 3:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1166>
Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/ldap.c | kbengine/ldap.c |
| Line | 918 | 963 |
| Object | attributes | attributes |

Code Snippet

File Name kbengine/ldap.c
Method */

```
....  
918.         if(!ludp->lud_attrs) {  
....  
963.
```

Double Free\Path 4:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1167 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 372 | 379 |
| Object | buf | buf |

Code Snippet

File Name kbengine/sds.c

Method sds sdscatvprintf(sds s, const char *fmt, va_list ap) {

```
....  
372.          free(buf);  
....  
379.          free(buf);
```

Double Free\Path 5:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1168 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 3287 | 3297 |
| Object | ubuf | ubuf |

Code Snippet

File Name kbengine/url.c

Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....  
3287.          free(ubuf);  
....  
3297.          free(ubuf);
```

Use of Uninitialized Variable

Query Path:

CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Variable\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1296 |
| Status | New |

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/mbedtls.c | kbengine/mbedtls.c |
| Line | 1027 | 1033 |
| Object | inputlen | inputlen |

Code Snippet

File Name kbengine/mbedtls.c
Method size_t inputlen,

```
....
1027.                                     size_t inputlen,
```

File Name kbengine/mbedtls.c
Method mbedtls_sha256(input, inputlen, sha256sum, 0);

```
....
1033.     mbedtls_sha256(input, inputlen, sha256sum, 0);
```

Use of Uninitialized Variable\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1297 |
| Status | New |

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 884 | 889 |
| Object | inputlen | inputlen |

Code Snippet

File Name kbengine/polarssl.c
Method size_t inputlen,

```
.....
884.                                     size_t inputlen,
```

File Name kbengine/polarssl.c
Method sha256(input, inputlen, sha256sum, 0);

```
.....
889.     sha256(input, inputlen, sha256sum, 0);
```

Use of Uninitialized Variable\Path 3:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1298>
Status New

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_srvr.c | kbengine/s3_srvr.c |
| Line | 2865 | 2899 |
| Object | Ttag | Ttag |

Code Snippet

File Name kbengine/s3_srvr.c
Method int ssl3_get_client_key_exchange(SSL *s)

```
.....
2865.         int Ttag, Tclass;
.....
2899.         n) != V_ASN1_CONSTRUCTED || Ttag != V_ASN1_SEQUENCE
```

Use of Uninitialized Variable\Path 4:

Severity Medium
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1299>
Status New

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_srvr.c | kbengine/s3_srvr.c |
| Line | 2865 | 2900 |
| Object | Tclass | Tclass |

Code Snippet

File Name kbengine/s3_srvr.c

Method int ssl3_get_client_key_exchange(SSL *s)

```
....
2865.         int Ttag, Tclass;
....
2900.         || Tclass != V_ASN1_UNIVERSAL) {
```

Inadequate Encryption Strength

Query Path:

CPP\Cx\CPP Medium Threat\Inadequate Encryption Strength Version:1

Categories

FISMA 2014: Configuration Management

NIST SP 800-53: SC-13 Cryptographic Protection (P1)

OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Inadequate Encryption Strength\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1548 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_auth_create_cram_md5_message at line 410 of kbengine/curl_sasl.c, to protect sensitive personal information passwd, from kbengine/curl_sasl.c at line 410.

| | Source | Destination |
|--------|----------------------|-----------------------------------|
| File | kbengine/curl_sasl.c | kbengine/curl_sasl.c |
| Line | 476 | 475 |
| Object | passwd | Curl_auth_create_cram_md5_message |

Code Snippet

File Name kbengine/curl_sasl.c
Method CURLcode Curl_sasl_continue(struct SASL *sasl, struct connectdata *conn,

```
....
476.                                     conn->passwd,
&resp, &len);
....
475.         result = Curl_auth_create_cram_md5_message(data, chlg, conn-
>user,
```

Inadequate Encryption Strength\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1549 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_auth_create_digest_md5_message at line 410 of kbengine/curl_sasl.c, to protect sensitive personal information passwd, from kbengine/curl_sasl.c at line 410.

| | Source | Destination |
|--------|----------------------|-------------------------------------|
| File | kbengine/curl_sasl.c | kbengine/curl_sasl.c |
| Line | 482 | 481 |
| Object | passwd | Curl_auth_create_digest_md5_message |

Code Snippet

File Name kbengine/curl_sasl.c

Method CURLcode Curl_sasl_continue(struct SASL *sasl, struct connectdata *conn,

```
....  
482.                                     conn->user, conn->  
>passwd,  
....  
481.     result = Curl_auth_create_digest_md5_message(data, serverdata,
```

Inadequate Encryption Strength\Path 3:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1550>

Status New

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 413 of kbengine/pop3.c, to protect sensitive personal information passwd, from kbengine/pop3.c at line 413.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/pop3.c | kbengine/pop3.c |
| Line | 439 | 438 |
| Object | passwd | Curl_MD5_update |

Code Snippet

File Name kbengine/pop3.c

Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....  
439.                                     curlx_uztoui(strlen(conn->passwd));  
....  
438.     Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

Inadequate Encryption Strength\Path 4:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1551>

Status New

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 413 of kbengine/pop3.c, to protect sensitive personal information passwd, from kbengine/pop3.c at line 413.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/pop3.c | kbengine/pop3.c |
| Line | 438 | 438 |
| Object | passwd | Curl_MD5_update |

Code Snippet

File Name kbengine/pop3.c

Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....  
438.      Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

Environment Injection

Query Path:

CPP\Cx\CPP Medium Threat\Environment Injection Version:0

Categories

OWASP Top 10 2013: A1-Injection

FISMA 2014: System And Information Integrity

NIST SP 800-53: SI-10 Information Input Validation (P1)

OWASP Top 10 2017: A1-Injection

Description

Environment Injection\Path 1:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1169>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/main.cpp | kbengine/main.cpp |
| Line | 304 | 324 |
| Object | getenv | setenv |

Code Snippet

File Name kbengine/main.cpp

Method int process_newassets(int argc, char* argv[], const std::string assetsType)

```
....  
304.      std::string res_path = getenv("KBE_RES_PATH") == NULL ? "" :  
getenv("KBE_RES_PATH");  
....  
324.      setenv("KBE_RES_PATH", res_path.c_str(), 1);
```

Environment Injection\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1170 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/main.cpp | kbengine/main.cpp |
| Line | 305 | 324 |
| Object | getenv | setenv |

Code Snippet

File Name kbengine/main.cpp

Method int process_newassets(int argc, char* argv[], const std::string assetsType)

```
....
305.         std::string root_path = getenv("KBE_ROOT") == NULL ? "" :
getenv("KBE_ROOT");
....
324.         setenv("KBE_RES_PATH", res_path.c_str(), 1);
```

Use of Hard coded Cryptographic Key

Query Path:

CPP\Cx\CPP Medium Threat\Use of Hard coded Cryptographic Key Version:0

Categories

FISMA 2014: Identification And Authentication

NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management (P1)

OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Hard coded Cryptographic Key\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1171 |
| Status | New |

The variable num_encrypted_key_bytes at line 373 of kbengine/s2_srvr.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/s2_srvr.c | kbengine/s2_srvr.c |
| Line | 498 | 498 |
| Object | num_encrypted_key_bytes | num_encrypted_key_bytes |

Code Snippet

File Name kbengine/s2_srvr.c

Method static int get_client_master_key(SSL *s)

```
.....
498.          num_encrypted_key_bytes = 8;
```

Use of Hard coded Cryptographic Key\Path 2:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1172 |
| Status | New |

The variable num_encrypted_key_bytes at line 373 of kbengine/s2_srvr.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/s2_srvr.c | kbengine/s2_srvr.c |
| Line | 500 | 500 |
| Object | num_encrypted_key_bytes | num_encrypted_key_bytes |

Code Snippet

File Name kbengine/s2_srvr.c
Method static int get_client_master_key(SSL *s)

```
.....
500.          num_encrypted_key_bytes = 5;
```

Use of a One Way Hash without a Salt

Query Path:

CPP\Cx\CPP Medium Threat\Use of a One Way Hash without a Salt Version:1

Categories

FISMA 2014: Media Protection

NIST SP 800-53: SC-13 Cryptographic Protection (P1)

Description

Use of a One Way Hash without a Salt\Path 1:

| | |
|----------------|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2133 |
| Status | New |

The application protects passwords with SHA1_Final in aesni_cbc_hmac_sha1_ctrl, of kbengine/e_aes_cbc_hmac_sha1.c at line 810, using a cryptographic hash Address. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

| | Source | Destination |
|------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 824 | 826 |

| Object | Address | SHA1_Final |
|--------|---------|------------|
|--------|---------|------------|

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static int aesni_cbc_hmac_sha1_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg,

```

.....
824.          SHA1_Init(&key->head);
.....
826.          SHA1_Final(hmac_key, &key->head);

```

Use of a One Way Hash without a Salt\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2134>

Status New

The application protects passwords with SHA256_Final in aesni_cbc_hmac_sha256_ctrl, of kbengine/e_aes_cbc_hmac_sha256.c at line 787, using a cryptographic hash Address. However, the code does not salt the hash with an unpredictable, random value, allowing an attacker to reverse the hash value.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 801 | 803 |
| Object | Address | SHA256_Final |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c

Method static int aesni_cbc_hmac_sha256_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg,

```

.....
801.          SHA256_Init(&key->head);
.....
803.          SHA256_Final(hmac_key, &key->head);

```

Boolean Overflow

Query Path:

CPP\Cx\CPP Integer Overflow\Boolean Overflow Version:0

Categories

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

FISMA 2014: System And Information Integrity

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Boolean Overflow\Path 1:

Severity Medium

Result State To Verify

Online Results <http://WIN->

BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=548

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 946 of kbengine/url.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 963 | 963 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/url.c

Method static bool extract_if_dead(struct connectdata *conn,

```
....
963.         dead = (state & CONNRESULT_DEAD);
```

Char Overflow

Query Path:

CPP\Cx\CPP Integer Overflow\Char Overflow Version:1

Categories

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

Description

Char Overflow\Path 1:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=549>

Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 344 of kbengine/a_int.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/a_int.c | kbengine/a_int.c |
| Line | 372 | 372 |
| Object | AssignExpr | AssignExpr |

Code Snippet

File Name kbengine/a_int.c

Method int ASN1_INTEGER_set(ASN1_INTEGER *a, long v)

```
....
372.         buf[i] = (int)d & 0xff;
```

Improper Resource Access Authorization

Query Path:

CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

Categories

FISMA 2014: Identification And Authentication

NIST SP 800-53: AC-3 Access Enforcement (P1)

OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1552 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1014 | 1014 |
| Object | fgets | fgets |

Code Snippet

File Name kbengine/cookie.c
Method static char *get_line(char *buf, int len, FILE *input)

```
....  
1014.      char *b = fgets(buf, len, input);
```

Improper Resource Access Authorization\Path 2:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1553 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1014 | 1014 |
| Object | buf | buf |

Code Snippet

File Name kbengine/cookie.c
Method static char *get_line(char *buf, int len, FILE *input)

```
....  
1014.      char *b = fgets(buf, len, input);
```


Improper Resource Access Authorization\Path 3:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1554 |
| Status | New |

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/blast.c | kbengine/blast.c |
| Line | 437 | 437 |
| Object | hold | hold |

Code Snippet

File Name kbengine/blast.c

Method local unsigned inf(void *how, unsigned char **buf)

```
....  
437.         return fread(hold, 1, CHUNK, (FILE *)how);
```

Improper Resource Access Authorization\Path 4:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1555 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |
| Line | 256 | 256 |
| Object | ptr | ptr |

Code Snippet

File Name kbengine/gtls.c

Method static gnutls_datum_t load_file(const char *file)

```
....  
256.     if(fread(ptr, 1, (size_t)filelen, f) < (size_t)filelen) {
```

Improper Resource Access Authorization\Path 5:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1556 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 156 | 156 |
| Object | buffer | buffer |

Code Snippet

File Name kbengine/tool_operate.c

Method static curl_off_t vms_realfilesize(const char *name,

```
....  
156.         ret_stat = fread(buffer, 1, sizeof(buffer), file);
```

Improper Resource Access Authorization\Path 6:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1557>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |
| Line | 924 | 924 |
| Object | buf | buf |

Code Snippet

File Name kbengine/vtls.c

Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....  
924.         if((int) fread(buf, size, 1, fp) != 1)
```

Improper Resource Access Authorization\Path 7:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1558>

Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 668 | 668 |
| Object | buf | buf |

Code Snippet

File Name kbengine/gskit.c
Method static int pipe_ssloverssl(struct connectdata *conn, int sockindex,

```
....  
668.          n = read(BACKEND->remotefd, buf, sizeof(buf));
```

Improper Resource Access Authorization\Path 8:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1559>
Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 1300 | 1300 |
| Object | buf | buf |

Code Snippet

File Name kbengine/gskit.c
Method static int Curl_gskit_shutdown(struct connectdata *conn, int sockindex)

```
....  
1300.          nread = read(conn->sock[sockindex], buf, sizeof(buf));
```

Improper Resource Access Authorization\Path 9:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1560>
Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/security.c | kbengine/security.c |
| Line | 241 | 241 |
| Object | buffer | buffer |

Code Snippet

File Name kbengine/security.c
Method static ssize_t sec_rcv(struct connectdata *conn, int sockindex,

```
....  
241.          return read(fd, buffer, len);
```

Improper Resource Access Authorization\Path 10:

Severity Low

| | |
|----------------|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1561 |
| Status | New |

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/mailer.cpp | kbengine/mailer.cpp |
| Line | 150 | 150 |
| Object | get | get |

Code Snippet

File Name kbengine/mailer.cpp

Method bool mailer::setmessageHTMLfile(const std::string& filename) {

```
....  
150.             char c = file.get();
```

Improper Resource Access Authorization\Path 11:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1562 |
| Status | New |

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/mailer.cpp | kbengine/mailer.cpp |
| Line | 151 | 151 |
| Object | get | get |

Code Snippet

File Name kbengine/mailer.cpp

Method bool mailer::setmessageHTMLfile(const std::string& filename) {

```
....  
151.             for(; file.good(); c = file.get()) {
```

Improper Resource Access Authorization\Path 12:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1563 |
| Status | New |

| | Source | Destination |
|------|---------------------|---------------------|
| File | kbengine/mailer.cpp | kbengine/mailer.cpp |

| | | |
|--------|-----|-----|
| Line | 870 | 870 |
| Object | get | get |

Code Snippet

File Name kbengine/mailer.cpp

Method bool mailer::attach(const std::string& filename) {

```
....  
870.             char c = file.get();
```

Improper Resource Access Authorization\Path 13:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1564>

Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/mailer.cpp | kbengine/mailer.cpp |
| Line | 871 | 871 |
| Object | get | get |

Code Snippet

File Name kbengine/mailer.cpp

Method bool mailer::attach(const std::string& filename) {

```
....  
871.             for(; file.good(); c = file.get()) {
```

Improper Resource Access Authorization\Path 14:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1565>

Status New

| | Source | Destination |
|--------|----------------------------|----------------------------|
| File | kbengine/apr_dbd_freetds.c | kbengine/apr_dbd_freetds.c |
| Line | 704 | 704 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/apr_dbd_freetds.c

Method static void dbd_freetds_init(apr_pool_t *pool)

```
....  
704.          fprintf(stderr, "regcomp failed: %s\n", errmsg);
```

Improper Resource Access Authorization\Path 15:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1566 |
| Status | New |

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/blast.c | kbengine/blast.c |
| Line | 455 | 455 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/blast.c
Method int main(void)

```
....  
455.          fprintf(stderr, "blast error: %d\n", ret);
```

Improper Resource Access Authorization\Path 16:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1567 |
| Status | New |

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/blast.c | kbengine/blast.c |
| Line | 461 | 461 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/blast.c
Method int main(void)

```
....  
461.          fprintf(stderr, "blast warning: %u unused bytes of  
input\n", left);
```

Improper Resource Access Authorization\Path 17:

| | |
|--------------|-----------|
| Severity | Low |
| Result State | To Verify |

| | |
|----------------|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1568 |
| Status | New |

| | Source | Destination |
|--------|------------------------|------------------------|
| File | kbengine/cacertinmem.c | kbengine/cacertinmem.c |
| Line | 112 | 112 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/cacertinmem.c

Method static CURLcode sslctx_function(CURL *curl, void *sslctx, void *parm)

```
....  
112.      fprintf(stderr, "error adding certificate\n");
```

Improper Resource Access Authorization\Path 18:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1569 |
| Status | New |

| | Source | Destination |
|--------|------------------------|------------------------|
| File | kbengine/cacertinmem.c | kbengine/cacertinmem.c |
| Line | 115 | 115 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/cacertinmem.c

Method static CURLcode sslctx_function(CURL *curl, void *sslctx, void *parm)

```
....  
115.      fprintf(stderr, "%s\n", errbuf);
```

Improper Resource Access Authorization\Path 19:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1570 |
| Status | New |

| | Source | Destination |
|------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |

| | | |
|--------|---------|---------|
| Line | 1510 | 1510 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/cookie.c

Method static int cookie_output(struct CookieInfo *c, const char *dumphere)

```
....  
1510.          fprintf(out, "#\n# Fatal libcurl error\n");
```

Improper Resource Access Authorization\Path 20:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1571>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1517 | 1517 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/cookie.c

Method static int cookie_output(struct CookieInfo *c, const char *dumphere)

```
....  
1517.          fprintf(out, "%s\n", format_ptr);
```

Improper Resource Access Authorization\Path 21:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1572>

Status New

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1028 | 1028 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/d1_both.c

Method int dtls1_read_failed(SSL *s, int code)


```
....  
1028.          fprintf(stderr, "invalid state reached %s:%d", __FILE__,  
__LINE__);
```

Improper Resource Access Authorization\Path 22:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1573 |
| Status | New |

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1100 | 1100 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/d1_both.c
Method int dtls1_retransmit_buffered_messages(SSL *s)

```
....  
1100.          fprintf(stderr, "dtls1_retransmit_message()  
failed\n");
```

Improper Resource Access Authorization\Path 23:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1574 |
| Status | New |

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 1200 | 1200 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_retransmit_message(SSL *s, unsigned short seq, unsigned long frag_off,

```
....  
1200.          fprintf(stderr, "retransmit: message %d non-existant\n",  
seq);
```

Improper Resource Access Authorization\Path 24:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1575 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 222 | 222 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/easy.c

Method static CURLcode global_init(long flags, bool memoryfuncs)

```
....  
222.          DEBUGF(fprintf(stderr, "Error: Curl_ssl_init failed\n"));
```

Improper Resource Access Authorization\Path 25:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1576 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 228 | 228 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/easy.c

Method static CURLcode global_init(long flags, bool memoryfuncs)

```
....  
228.          DEBUGF(fprintf(stderr, "Error: win32_init failed\n"));
```

Improper Resource Access Authorization\Path 26:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1577 |
| Status | New |

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

| | | |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 234 | 234 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/easy.c

Method static CURLcode global_init(long flags, bool memoryfuncs)

```
....  
234.          DEBUGF(fprintf(stderr, "Error: Curl_amiga_init failed\n"));
```

Improper Resource Access Authorization\Path 27:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1578>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 241 | 241 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/easy.c

Method static CURLcode global_init(long flags, bool memoryfuncs)

```
....  
241.          DEBUGF(fprintf(stderr, "Warning: LONG namespace not  
available\n"));
```

Improper Resource Access Authorization\Path 28:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1579>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 246 | 246 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/easy.c

Method static CURLcode global_init(long flags, bool memoryfuncs)

```
....  
246.         DEBUGF(fprintf(stderr, "Error: resolver_global_init  
failed\n"));
```

Improper Resource Access Authorization\Path 29:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1580>
Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 254 | 254 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/easy.c
Method static CURLcode global_init(long flags, bool memoryfuncs)

```
....  
254.         DEBUGF(fprintf(stderr, "Error: libssh2_init failed\n"));
```

Improper Resource Access Authorization\Path 30:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1581>
Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 261 | 261 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/easy.c
Method static CURLcode global_init(long flags, bool memoryfuncs)

```
....  
261.         DEBUGF(fprintf(stderr, "Error: libssh_init failed\n"));
```

Improper Resource Access Authorization\Path 31:

Severity Low

| | |
|----------------|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1582 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 364 | 364 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/easy.c

Method struct Curl_easy *curl_easy_init(void)

```
....  
364.          DEBUGF(fprintf(stderr, "Error: curl_global_init failed\n"));
```

Improper Resource Access Authorization\Path 32:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1583 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 372 | 372 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/easy.c

Method struct Curl_easy *curl_easy_init(void)

```
....  
372.          DEBUGF(fprintf(stderr, "Error: Curl_open failed\n"));
```

Improper Resource Access Authorization\Path 33:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1584 |
| Status | New |

| | Source | Destination |
|------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |

| | | |
|--------|---------|---------|
| Line | 69 | 69 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/gtls.c

Method static void tls_log_func(int level, const char *str)

```
....  
69.      fprintf(stderr, "|<%d>| %s", level, str);
```

Improper Resource Access Authorization\Path 34:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1585>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/lib542.c | kbengine/lib542.c |
| Line | 40 | 40 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/lib542.c

Method int test(char *URL)

```
....  
40.      fprintf(stderr, "curl_global_init() failed\n");
```

Improper Resource Access Authorization\Path 35:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1586>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/lib542.c | kbengine/lib542.c |
| Line | 47 | 47 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/lib542.c

Method int test(char *URL)

```
....  
47.      fprintf(stderr, "curl_easy_init() failed\n");
```

Improper Resource Access Authorization\Path 36:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1587 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/mem.c | kbengine/mem.c |
| Line | 296 | 296 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/mem.c
Method void *CRYPTO_malloc_locked(int num, const char *file, int line)

```
....  
296.      fprintf(stderr, "LEVITTE_DEBUG_MEM:          > 0x%p (%d)\n",  
ret, num);
```

Improper Resource Access Authorization\Path 37:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1588 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/mem.c | kbengine/mem.c |
| Line | 321 | 321 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/mem.c
Method void CRYPTO_free_locked(void *str)

```
....  
321.      fprintf(stderr, "LEVITTE_DEBUG_MEM:          < 0x%p\n", str);
```

Improper Resource Access Authorization\Path 38:

| | |
|--------------|-----------|
| Severity | Low |
| Result State | To Verify |

| | |
|----------------|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1589 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/mem.c | kbengine/mem.c |
| Line | 344 | 344 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/mem.c

Method void *CRYPTO_malloc(int num, const char *file, int line)

```
....  
344.      fprintf(stderr, "LEVITTE_DEBUG_MEM:          > 0x%p (%d)\n",  
ret, num);
```

Improper Resource Access Authorization\Path 39:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1590 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/mem.c | kbengine/mem.c |
| Line | 389 | 389 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/mem.c

Method void *CRYPTO_realloc(void *str, int num, const char *file, int line)

```
....  
389.      fprintf(stderr, "LEVITTE_DEBUG_MEM:          | 0x%p -> 0x%p  
(%d)\n", str,
```

Improper Resource Access Authorization\Path 40:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1591 |
| Status | New |

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

| | | |
|--------|----------------|----------------|
| File | kbengine/mem.c | kbengine/mem.c |
| Line | 425 | 425 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/mem.c

Method void *CRYPTO_realloc_clean(void *str, int old_len, int num, const char *file,

```
....  
425.      fprintf(stderr,
```

Improper Resource Access Authorization\Path 41:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1592>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/mem.c | kbengine/mem.c |
| Line | 440 | 440 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/mem.c

Method void CRYPTO_free(void *str)

```
....  
440.      fprintf(stderr, "LEVITTE_DEBUG_MEM:          < 0x%p\n", str);
```

Improper Resource Access Authorization\Path 42:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1593>

Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 3153 | 3153 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/multi.c

Method void Curl_multi_dump(struct Curl_multi *multi)

```
....  
3153.      fprintf(stderr, "* Multi status: %d handles, %d alive\n",
```

Improper Resource Access Authorization\Path 43:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1594 |
| Status | New |

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 3158 | 3158 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/multi.c
Method void Curl_multi_dump(struct Curl_multi *multi)

```
....  
3158.      fprintf(stderr, "handle %p, state %s, %d sockets\n",
```

Improper Resource Access Authorization\Path 44:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1595 |
| Status | New |

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 3165 | 3165 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/multi.c
Method void Curl_multi_dump(struct Curl_multi *multi)

```
....  
3165.      fprintf(stderr, "%d ", (int)s);
```

Improper Resource Access Authorization\Path 45:

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

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1596](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1596)

Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 3167 | 3167 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/multi.c

Method void Curl_multi_dump(struct Curl_multi *multi)

```
....  
3167.          fprintf(stderr, "INTERNAL CONFUSION\n");
```

Improper Resource Access Authorization\Path 46:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1597>

Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 3170 | 3170 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/multi.c

Method void Curl_multi_dump(struct Curl_multi *multi)

```
....  
3170.          fprintf(stderr, "[%s %s] ",
```

Improper Resource Access Authorization\Path 47:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1598>

Status New

| | Source | Destination |
|------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 3175 | 3175 |

| | | |
|--------|---------|---------|
| Object | fprintf | fprintf |
|--------|---------|---------|

Code Snippet

File Name kbengine/multi.c

Method void Curl_multi_dump(struct Curl_multi *multi)

```
....
3175.          fprintf(stderr, "\n");
```

Improper Resource Access Authorization\Path 48:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1599>

Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/rsa_sign.c | kbengine/rsa_sign.c |
| Line | 259 | 259 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/rsa_sign.c

Method int int_rsa_verify(int dtype, const unsigned char *m,

```
....
259.          fprintf(stderr, "in(%s) expect(%s)\n",
OBJ_nid2ln(sigtype),
```

Improper Resource Access Authorization\Path 49:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1600>

Status New

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_clnt.c | kbengine/s3_clnt.c |
| Line | 1290 | 1290 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/s3_clnt.c

Method int ssl3_get_server_certificate(SSL *s)

```
....
1290.      fprintf(stderr, "pkey,x = %p, %p\n", pkey, x);
```

Improper Resource Access Authorization\Path 50:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=1601 |
| Status | New |

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_clnt.c | kbengine/s3_clnt.c |
| Line | 1291 | 1291 |
| Object | fprintf | fprintf |

Code Snippet

File Name kbengine/s3_clnt.c
Method int ssl3_get_server_certificate(SSL *s)

```
....
1291.      fprintf(stderr, "ssl_cert_type(x,pkey) = %d\n",
ssl_cert_type(x, pkey));
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

NULL Pointer Dereference\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2243 |
| Status | New |

The variable declared in null at kbengine/a_bytes.c in line 245 is not initialized when it is used by data at kbengine/a_bytes.c in line 245.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/a_bytes.c | kbengine/a_bytes.c |
| Line | 247 | 283 |
| Object | null | data |

Code Snippet

File Name kbengine/a_bytes.c

Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

```
....
247.         ASN1_STRING *os = NULL;
....
283.         memcpy(&(b.data[num]), os->data, os->length);
```

NULL Pointer Dereference\Path 2:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2244>

Status New

The variable declared in null at kbengine/apr_snprintf.c in line 683 is not initialized when it is used by s at kbengine/apr_snprintf.c in line 683.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 1021 | 1331 |
| Object | null | s |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....
1021.         s = NULL;
....
1331.         INS_CHAR(*s, sp, bep, cc);
```

NULL Pointer Dereference\Path 3:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2245>

Status New

The variable declared in null at kbengine/apr_snprintf.c in line 683 is not initialized when it is used by s at kbengine/apr_snprintf.c in line 683.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 1021 | 1318 |
| Object | null | s |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....
1021.                s = NULL;
....
1318.                INS_CHAR(*s, sp, bep, cc);
```

NULL Pointer Dereference\Path 4:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2246>

Status New

The variable declared in null at kbengine/blast.c in line 446 is not initialized when it is used by in at kbengine/blast.c in line 383.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/blast.c | kbengine/blast.c |
| Line | 453 | 394 |
| Object | null | in |

Code Snippet

File Name kbengine/blast.c

Method int main(void)

```
....
453.    ret = blast(inf, stdin, outf, stdout, &left, NULL);
```



File Name kbengine/blast.c

Method int blast(blast_in infun, void *inhow, blast_out outfun, void *outhow,

```
....
394.    s.in = *in;
```

NULL Pointer Dereference\Path 5:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2247>

Status New

The variable declared in null at kbengine/blast.c in line 446 is not initialized when it is used by in at kbengine/blast.c in line 383.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/blast.c | kbengine/blast.c |
| Line | 453 | 394 |
| Object | null | in |

Code Snippet

File Name kbengine/blast.c

Method int main(void)

```
....
453.         ret = blast(inf, stdin, outf, stdout, &left, NULL);
```



File Name kbengine/blast.c

Method int blast(blast_in infun, void *inhow, blast_out outfun, void *outhow,

```
....
394.         s.in = *in;
```

NULL Pointer Dereference\Path 6:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2248>

Status New

The variable declared in null at kbengine/connect.c in line 241 is not initialized when it is used by addr at kbengine/connect.c in line 241.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/connect.c | kbengine/connect.c |
| Line | 254 | 369 |
| Object | null | addr |

Code Snippet

File Name kbengine/connect.c

Method static CURLcode bindlocal(struct connectdata *conn,

```
....
254.         struct Curl_dns_entry *h = NULL;
....
369.         dev, af, myhost, h->addr->ai_family);
```

NULL Pointer Dereference\Path 7:

Severity Low

Result State To Verify

Online Results [http://WIN-](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2248)

BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2249

Status New

The variable declared in null at kbengine/cookie.c in line 1215 is not initialized when it is used by expirestr at kbengine/cookie.c in line 104.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1222 | 106 |
| Object | null | expirestr |

Code Snippet

File Name kbengine/cookie.c

Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....  
1222.    struct Cookie *mainco = NULL;
```

File Name kbengine/cookie.c

Method static void freecookie(struct Cookie *co)

```
....  
106.    free(co->expirestr);
```

NULL Pointer Dereference\Path 8:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2250>

Status New

The variable declared in null at kbengine/cookie.c in line 1215 is not initialized when it is used by domain at kbengine/cookie.c in line 104.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1222 | 107 |
| Object | null | domain |

Code Snippet

File Name kbengine/cookie.c

Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....  
1222.    struct Cookie *mainco = NULL;
```

File Name kbengine/cookie.c
Method static void freecookie(struct Cookie *co)

```
....  
107.     free(co->domain);
```

NULL Pointer Dereference\Path 9:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2251>
Status New

The variable declared in null at kbengine/cookie.c in line 1215 is not initialized when it is used by path at kbengine/cookie.c in line 104.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1222 | 108 |
| Object | null | path |

Code Snippet

File Name kbengine/cookie.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....  
1222.     struct Cookie *mainco = NULL;
```

File Name kbengine/cookie.c
Method static void freecookie(struct Cookie *co)

```
....  
108.     free(co->path);
```

NULL Pointer Dereference\Path 10:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2252>
Status New

The variable declared in null at kbengine/cookie.c in line 1215 is not initialized when it is used by spath at kbengine/cookie.c in line 104.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1222 | 109 |
| Object | null | spath |

Code Snippet

File Name kbengine/cookie.c

Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1222.    struct Cookie *mainco = NULL;
```



File Name kbengine/cookie.c

Method static void freecookie(struct Cookie *co)

```
....
109.    free(co->spath);
```

NULL Pointer Dereference\Path 11:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2253>

Status New

The variable declared in null at kbengine/cookie.c in line 1215 is not initialized when it is used by name at kbengine/cookie.c in line 104.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1222 | 110 |
| Object | null | name |

Code Snippet

File Name kbengine/cookie.c

Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1222.    struct Cookie *mainco = NULL;
```



File Name kbengine/cookie.c

Method static void freecookie(struct Cookie *co)

```
....
110.    free(co->name);
```

NULL Pointer Dereference\Path 12:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2254 |
| Status | New |

The variable declared in null at kbengine/cookie.c in line 1215 is not initialized when it is used by value at kbengine/cookie.c in line 104.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1222 | 111 |
| Object | null | value |

Code Snippet

File Name kbengine/cookie.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1222.    struct Cookie *mainco = NULL;
```

File Name kbengine/cookie.c
Method static void freecookie(struct Cookie *co)

```
....
111.    free(co->value);
```

NULL Pointer Dereference\Path 13:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2255 |
| Status | New |

The variable declared in null at kbengine/cookie.c in line 1215 is not initialized when it is used by maxage at kbengine/cookie.c in line 104.

| | Source | Destination |
|------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1222 | 112 |

| | | |
|--------|------|--------|
| Object | null | maxage |
|--------|------|--------|

Code Snippet

File Name kbengine/cookie.c

Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1222.    struct Cookie *mainco = NULL;
```

File Name kbengine/cookie.c

Method static void freecookie(struct Cookie *co)

```
....
112.    free(co->maxage);
```

NULL Pointer Dereference\Path 14:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2256>

Status New

The variable declared in null at kbengine/cookie.c in line 1215 is not initialized when it is used by version at kbengine/cookie.c in line 104.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1222 | 113 |
| Object | null | version |

Code Snippet

File Name kbengine/cookie.c

Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1222.    struct Cookie *mainco = NULL;
```

File Name kbengine/cookie.c

Method static void freecookie(struct Cookie *co)

```
....
113.    free(co->version);
```

NULL Pointer Dereference\Path 15:

Severity Low

| | |
|----------------|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2257 |
| Status | New |

The variable declared in null at kbengine/d1_both.c in line 647 is not initialized when it is used by reassembly at kbengine/d1_both.c in line 647.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 679 | 721 |
| Object | null | reassembly |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr, int *ok)

```
....  
679.             frag = NULL;  
....  
721.             OPENSSL_free(frag->reassembly);
```

NULL Pointer Dereference\Path 16:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2258 |
| Status | New |

The variable declared in null at kbengine/d1_both.c in line 647 is not initialized when it is used by reassembly at kbengine/d1_both.c in line 647.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_both.c | kbengine/d1_both.c |
| Line | 679 | 689 |
| Object | null | reassembly |

Code Snippet

File Name kbengine/d1_both.c
Method dtls1_reassemble_fragment(SSL *s, const struct hm_header_st *msg_hdr, int *ok)

```
....  
679.             frag = NULL;  
....  
689.             if (frag->reassembly == NULL) {
```

NULL Pointer Dereference\Path 17:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2259 |
| Status | New |

The variable declared in null at kbengine/e_aes.c in line 269 is not initialized when it is used by cbc at kbengine/e_aes.c in line 269.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 281 | 280 |
| Object | null | cbc |

Code Snippet

File Name kbengine/e_aes.c

Method static int aesni_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....  
281.             (cbc128_f) aesni_cbc_encrypt : NULL;  
....  
280.             dat->stream.cbc = mode == EVP_CIPH_CBC_MODE ?
```

NULL Pointer Dereference\Path 18:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2260 |
| Status | New |

The variable declared in null at kbengine/e_aes.c in line 923 is not initialized when it is used by cbc at kbengine/e_aes.c in line 923.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 955 | 954 |
| Object | null | cbc |

Code Snippet

File Name kbengine/e_aes.c

Method static int aes_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....  
955.             (cbc128_f) vpaes_cbc_encrypt : NULL;  
....  
954.             dat->stream.cbc = mode == EVP_CIPH_CBC_MODE ?
```

NULL Pointer Dereference\Path 19:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2261 |
| Status | New |

The variable declared in null at kbengine/e_aes.c in line 923 is not initialized when it is used by cbc at kbengine/e_aes.c in line 923.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 962 | 961 |
| Object | null | cbc |

Code Snippet

File Name kbengine/e_aes.c

Method static int aes_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
962.                (cbc128_f) AES_cbc_encrypt : NULL;
....
961.                dat->stream.cbc = mode == EVP_CIPH_CBC_MODE ?
```

NULL Pointer Dereference\Path 20:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2262 |
| Status | New |

The variable declared in null at kbengine/e_aes.c in line 923 is not initialized when it is used by cbc at kbengine/e_aes.c in line 923.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 994 | 993 |
| Object | null | cbc |

Code Snippet

File Name kbengine/e_aes.c

Method static int aes_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
994.                (cbc128_f) vpaes_cbc_encrypt : NULL;
....
993.                dat->stream.cbc = mode == EVP_CIPH_CBC_MODE ?
```


NULL Pointer Dereference\Path 21:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2263 |
| Status | New |

The variable declared in null at kbengine/e_aes.c in line 923 is not initialized when it is used by cbc at kbengine/e_aes.c in line 923.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 1001 | 1000 |
| Object | null | cbc |

Code Snippet

File Name kbengine/e_aes.c

Method static int aes_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....  
1001.          (cbc128_f) AES_cbc_encrypt : NULL;  
....  
1000.          dat->stream.cbc = mode == EVP_CIPH_CBC_MODE ?
```

NULL Pointer Dereference\Path 22:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2264 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 683 is not initialized when it is used by handle at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 692 | 692 |
| Object | null | handle |

Code Snippet

File Name kbengine/gskit.c

Method static void close_one(struct ssl_connect_data *connssl,

```
....  
692.          BACKEND->handle = (gsk_handle) NULL;
```

NULL Pointer Dereference\Path 23:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2265 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 683 is not initialized when it is used by backend at kbengine/gskit.c in line 508.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 692 | 510 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c

Method static void close_one(struct ssl_connect_data *connssl,

```
....  
692.     BACKEND->handle = (gsk_handle) NULL;
```



File Name kbengine/gskit.c

Method static void close_async_handshake(struct ssl_connect_data *connssl)

```
....  
510.     QsoDestroyIOCompletionPort (BACKEND->iocport);
```

NULL Pointer Dereference\Path 24:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2266 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 508.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 510 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c

Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```
....
818.     BACKEND->handle = (gsk_handle) NULL;
```

File Name kbengine/gskit.c

Method static void close_async_handshake(struct ssl_connect_data *connssl)

```
....
510.     QsoDestroyIOCompletionPort (BACKEND->iocport);
```

NULL Pointer Dereference\Path 25:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2267>

Status New

The variable declared in null at kbengine/gskit.c in line 683 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 692 | 702 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c

Method static void close_one(struct ssl_connect_data *connssl,

```
....
692.     BACKEND->handle = (gsk_handle) NULL;
....
702.     if (BACKEND->iocport >= 0)
```

NULL Pointer Dereference\Path 26:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2268>

Status New

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |

| | | |
|--------|------|---------|
| Line | 818 | 702 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c

Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```
....
818.     BACKEND->handle = (gsk_handle) NULL;
```

File Name kbengine/gskit.c

Method static void close_one(struct ssl_connect_data *connssl,

```
....
702.     if (BACKEND->iocport >= 0)
```

NULL Pointer Dereference\Path 27:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2269>

Status New

The variable declared in null at kbengine/gskit.c in line 683 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 692 | 698 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c

Method static void close_one(struct ssl_connect_data *connssl,

```
....
692.     BACKEND->handle = (gsk_handle) NULL;
....
698.     close (BACKEND->remotefd);
```

NULL Pointer Dereference\Path 28:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2270>

Status New

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 698 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c

Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```
....
818.     BACKEND->handle = (gsk_handle) NULL;
```

File Name kbengine/gskit.c

Method static void close_one(struct ssl_connect_data *connssl,

```
....
698.     close(BACKEND->remotefd);
```

NULL Pointer Dereference\Path 29:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2271>

Status New

The variable declared in null at kbengine/gskit.c in line 683 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 692 | 697 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c

Method static void close_one(struct ssl_connect_data *connssl,

```
....
692.     BACKEND->handle = (gsk_handle) NULL;
....
697.     if (BACKEND->remotefd >= 0) {
```

NULL Pointer Dereference\Path 30:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2272 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 697 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```
....
818.     BACKEND->handle = (gsk_handle) NULL;
```

File Name kbengine/gskit.c
Method static void close_one(struct ssl_connect_data *connssl,

```
....
697.     if (BACKEND->remotefd >= 0) {
```

NULL Pointer Dereference\Path 31:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2273 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 683 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 692 | 694 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static void close_one(struct ssl_connect_data *connssl,

```
....
692.         BACKEND->handle = (gsk_handle) NULL;
....
694.         close (BACKEND->localfd);
```

NULL Pointer Dereference\Path 32:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2274 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 694 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```
....
818.         BACKEND->handle = (gsk_handle) NULL;
```

File Name kbengine/gskit.c
Method static void close_one(struct ssl_connect_data *connssl,

```
....
694.         close (BACKEND->localfd);
```

NULL Pointer Dereference\Path 33:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2275 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 683 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |

| | | |
|--------|------|---------|
| Line | 692 | 693 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c

Method static void close_one(struct ssl_connect_data *connssl,

```
....
692.     BACKEND->handle = (gsk_handle) NULL;
693.     if (BACKEND->localfd >= 0) {
```

NULL Pointer Dereference\Path 34:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2276>

Status New

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 693 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c

Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```
....
818.     BACKEND->handle = (gsk_handle) NULL;
```

File Name kbengine/gskit.c

Method static void close_one(struct ssl_connect_data *connssl,

```
....
693.     if (BACKEND->localfd >= 0) {
```

NULL Pointer Dereference\Path 35:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2277>

Status New

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by handle at kbengine/gskit.c in line 795.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 818 |
| Object | null | handle |

Code Snippet

File Name kbengine/gskit.c

Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```
....  
818.     BACKEND->handle = (gsk_handle) NULL;
```

NULL Pointer Dereference\Path 36:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2278>

Status New

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 687 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c

Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```
....  
818.     BACKEND->handle = (gsk_handle) NULL;
```



File Name kbengine/gskit.c

Method static void close_one(struct ssl_connect_data *connssl,

```
....  
687.     gskit_status(conn->data, gsk_secure_soc_close(&BACKEND->handle),
```

NULL Pointer Dereference\Path 37:

Severity Low

| | |
|----------------|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2279 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 683.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 686 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```
....
818.     BACKEND->handle = (gsk_handle) NULL;
```



File Name kbengine/gskit.c
Method static void close_one(struct ssl_connect_data *connssl,

```
....
686.     if (BACKEND->handle) {
```

NULL Pointer Dereference\Path 38:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2280 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 795.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 982 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```

.....
818.     BACKEND->handle = (gsk_handle) NULL;
.....
982.     if (BACKEND->iocport != -1) {

```

NULL Pointer Dereference\Path 39:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2281 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 795.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 875 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```

.....
818.     BACKEND->handle = (gsk_handle) NULL;
.....
875.     curlx_nonblock(BACKEND->remotefd, TRUE);

```

NULL Pointer Dereference\Path 40:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2282 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 795.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 874 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```

.....
818.     BACKEND->handle = (gsk_handle) NULL;
.....
874.     curlx_nonblock(BACKEND->localfd, TRUE);

```

NULL Pointer Dereference\Path 41:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2283 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 795.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 872 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```

.....
818.     BACKEND->handle = (gsk_handle) NULL;
.....
872.     setsockopt(BACKEND->remoteafd, SOL_SOCKET, SO_SNDBUF,

```

NULL Pointer Dereference\Path 42:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2284 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 795.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 870 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```

.....
818.     BACKEND->handle = (gsk_handle) NULL;
.....
870.     setsockopt (BACKEND->localfd, SOL_SOCKET, SO_SNDBUF,

```

NULL Pointer Dereference\Path 43:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2285 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 795.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 868 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```

.....
818.     BACKEND->handle = (gsk_handle) NULL;
.....
868.     setsockopt (BACKEND->remoteFd, SOL_SOCKET, SO_RCVBUF,

```

NULL Pointer Dereference\Path 44:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2286 |
| Status | New |

The variable declared in null at kbengine/gskit.c in line 795 is not initialized when it is used by backend at kbengine/gskit.c in line 795.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 818 | 866 |
| Object | null | backend |

Code Snippet

File Name kbengine/gskit.c
Method static CURLcode gskit_connect_step1(struct connectdata *conn, int sockindex)

```

.....
818.      BACKEND->handle = (gsk_handle) NULL;
.....
866.      setsockopt (BACKEND->localfd, SOL_SOCKET, SO_RCVBUF,

```

NULL Pointer Dereference\Path 45:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2287 |
| Status | New |

The variable declared in null at kbengine/multi.c in line 2497 is not initialized when it is used by time at kbengine/multi.c in line 2497.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 2504 | 2531 |
| Object | null | time |

Code Snippet

File Name kbengine/multi.c
Method static CURLMcode add_next_timeout(struct curltime now,

```

.....
2504.      struct time_node *node = NULL;
.....
2531.      memcpy(tv, &node->time, sizeof(*tv));

```

NULL Pointer Dereference\Path 46:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2288 |
| Status | New |

The variable declared in null at kbengine/pk7_lib.c in line 605 is not initialized when it is used by flags at kbengine/pk7_lib.c in line 605.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/pk7_lib.c | kbengine/pk7_lib.c |
| Line | 635 | 642 |
| Object | null | flags |

Code Snippet

File Name kbengine/pk7_lib.c
Method int PKCS7_stream(unsigned char ***boundary, PKCS7 *p7)

```

.....
635.          os = NULL;
.....
642.          os->flags |= ASN1_STRING_FLAG_NDEF;

```

NULL Pointer Dereference\Path 47:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2289 |
| Status | New |

The variable declared in null at kbengine/s23_clnt.c in line 146 is not initialized when it is used by init_buf at kbengine/s23_clnt.c in line 146.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/s23_clnt.c | kbengine/s23_clnt.c |
| Line | 199 | 189 |
| Object | null | init_buf |

Code Snippet

File Name kbengine/s23_clnt.c
Method int ssl23_connect(SSL *s)

```

.....
199.          buf = NULL;
.....
189.          if (s->init_buf == NULL) {

```

NULL Pointer Dereference\Path 48:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2290 |
| Status | New |

The variable declared in null at kbengine/s3_clnt.c in line 893 is not initialized when it is used by cipher at kbengine/s3_clnt.c in line 893.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_clnt.c | kbengine/s3_clnt.c |
| Line | 1002 | 1008 |
| Object | null | cipher |

Code Snippet

File Name kbengine/s3_clnt.c
Method int ssl3_get_server_hello(SSL *s)

```

.....
1002.          SSL_CIPHER *pref_cipher = NULL;
.....
1008.          s->session->cipher = pref_cipher ?

```

NULL Pointer Dereference\Path 49:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2291 |
| Status | New |

The variable declared in null at kbengine/s3_clnt.c in line 893 is not initialized when it is used by session at kbengine/s3_clnt.c in line 893.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_clnt.c | kbengine/s3_clnt.c |
| Line | 1002 | 1118 |
| Object | null | session |

Code Snippet

File Name kbengine/s3_clnt.c
Method int ssl3_get_server_hello(SSL *s)

```

.....
1002.          SSL_CIPHER *pref_cipher = NULL;
.....
1118.          if (s->session->compress_meth != 0) {

```

NULL Pointer Dereference\Path 50:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2292 |
| Status | New |

The variable declared in null at kbengine/s3_clnt.c in line 893 is not initialized when it is used by session at kbengine/s3_clnt.c in line 893.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/s3_clnt.c | kbengine/s3_clnt.c |
| Line | 1002 | 1086 |
| Object | null | session |

Code Snippet

File Name kbengine/s3_clnt.c
Method int ssl3_get_server_hello(SSL *s)


```
.....
1002.          SSL_CIPHER *pref_cipher = NULL;
.....
1086.          if (s->hit && (s->session->cipher_id != c->id)) {
```

Unchecked Array Index

Query Path:

CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unchecked Array Index\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2520 |
| Status | New |

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/bn_gf2m.c | kbengine/bn_gf2m.c |
| Line | 452 | 452 |
| Object | n | n |

Code Snippet

File Name kbengine/bn_gf2m.c
Method int BN_GF2m_mod_arr(BIGNUM *r, const BIGNUM *a, const int p[])

```
.....
452.          z[n] ^= (zz << d0);
```

Unchecked Array Index\Path 2:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2521 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 726 | 726 |
| Object | pathlen | pathlen |

Code Snippet

File Name kbengine/cookie.c

Method Curl_cookie_add(struct Curl_easy *data,

```
....  
726.          co->path[pathlen] = 0; /* zero terminate */
```

Unchecked Array Index\Path 3:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2522>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 999 | 999 |
| Object | myhash | myhash |

Code Snippet

File Name kbengine/cookie.c

Method Curl_cookie_add(struct Curl_easy *data,

```
....  
999.          c->cookies[myhash] = co;
```

Unchecked Array Index\Path 4:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2523>

Status New

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 182 | 182 |
| Object | pathLength | pathLength |

Code Snippet

File Name kbengine/curl_path.c

Method CURLcode Curl_get_pathname(const char **cpp, char **path, char *homedir)

```
....  
182.          (*path)[pathLength] = '\\0';
```

Unchecked Array Index\Path 5:

Severity Low

Result State To Verify

| | |
|----------------|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2524 |
| Status | New |

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 188 | 188 |
| Object | pathLength | pathLength |

Code Snippet

File Name kbengine/curl_path.c

Method CURLcode Curl_get_pathname(const char **cpp, char **path, char *homedir)

```
....  
188.      (*path)[pathLength] = '\\0';
```

Unchecked Array Index\Path 6:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2525 |
| Status | New |

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 71 | 71 |
| Object | homelen | homelen |

Code Snippet

File Name kbengine/curl_path.c

Method CURLcode Curl_getworkingpath(struct connectdata *conn,

```
....  
71.      real_path[homelen] = '/';
```

Unchecked Array Index\Path 7:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2526 |
| Status | New |

| | Source | Destination |
|------|-------------------|-------------------|
| File | kbengine/cyassl.c | kbengine/cyassl.c |

| | | |
|--------|-----------|-----------|
| Line | 479 | 479 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/cyassl.c

Method cyassl_connect_step2(struct connectdata *conn,

```
....  
479.     conn->recv[sockindex] = cyassl_recv;
```

Unchecked Array Index\Path 8:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2527>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cyassl.c | kbengine/cyassl.c |
| Line | 480 | 480 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/cyassl.c

Method cyassl_connect_step2(struct connectdata *conn,

```
....  
480.     conn->send[sockindex] = cyassl_send;
```

Unchecked Array Index\Path 9:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2528>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cyassl.c | kbengine/cyassl.c |
| Line | 925 | 925 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/cyassl.c

Method cyassl_connect_common(struct connectdata *conn,

```
....  
925.         conn->recv[sockindex] = cyassl_recv;
```

Unchecked Array Index\Path 10:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2529 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cyassl.c | kbengine/cyassl.c |
| Line | 926 | 926 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/cyassl.c
Method cyassl_connect_common(struct connectdata *conn,

```
....  
926.         conn->send[sockindex] = cyassl_send;
```

Unchecked Array Index\Path 11:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2530 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/dict.c | kbengine/dict.c |
| Line | 120 | 120 |
| Object | olen | olen |

Code Snippet

File Name kbengine/dict.c
Method static char *unescape_word(struct Curl_easy *data, const char *inputbuff)

```
....  
120.         dictp[olen] = 0;
```

Unchecked Array Index\Path 12:

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

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2531](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2531)

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/escape.c | kbengine/escape.c |
| Line | 131 | 131 |
| Object | strindex | strindex |

Code Snippet

File Name kbengine/escape.c

Method char *curl_easy_escape(struct Curl_easy *data, const char *string,

```
....  
131.     ns[strindex] = 0; /* terminate it */
```

Unchecked Array Index\Path 13:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2532>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/escape.c | kbengine/escape.c |
| Line | 193 | 193 |
| Object | strindex | strindex |

Code Snippet

File Name kbengine/escape.c

Method CURLcode Curl_urldecode(struct Curl_easy *data,

```
....  
193.     ns[strindex] = 0; /* terminate it */
```

Unchecked Array Index\Path 14:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2533>

Status New

| | Source | Destination |
|------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 856 | 856 |

| | | |
|--------|---|---|
| Object | s | s |
|--------|---|---|

Code Snippet

File Name kbengine/ftp.c

Method static int ftp_domore_getsock(struct connectdata *conn, curl_socket_t *socks,

```
....  
856.          socks[s] = conn->tempsock[i];
```

Unchecked Array Index\Path 15:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2534>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |
| Line | 1411 | 1411 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/gtls.c

Method gtls_connect_step3(struct connectdata *conn,

```
....  
1411.      conn->recv[sockindex] = gtls_recv;
```

Unchecked Array Index\Path 16:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2535>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |
| Line | 1412 | 1412 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/gtls.c

Method gtls_connect_step3(struct connectdata *conn,

```
.....
1412.      conn->send[sockindex] = gtls_send;
```

Unchecked Array Index\Path 17:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2536 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 254 | 254 |
| Object | len | len |

Code Snippet

File Name kbengine/http.c
Method char *Curl_copy_header_value(const char *header)

```
.....
254.      value[len] = 0; /* zero terminate */
```

Unchecked Array Index\Path 18:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2537 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1027 | 1027 |
| Object | len | len |

Code Snippet

File Name kbengine/imap.c
Method static CURLcode imap_state_listsearch_resp(struct connectdata *conn,

```
.....
1027.      line[len] = '\n';
```

Unchecked Array Index\Path 19:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2538 |

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2538](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2538)

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1029 | 1029 |
| Object | len | len |

Code Snippet

File Name kbengine/imap.c

Method static CURLcode imap_state_listsearch_resp(struct connectdata *conn,

```
....  
1029.     line[len] = '\0';
```

Unchecked Array Index\Path 20:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2539>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1840 | 1840 |
| Object | newlen | newlen |

Code Snippet

File Name kbengine/imap.c

Method static char *imap_atom(const char *str, bool escape_only)

```
....  
1840.     newstr[newlen] = '\0';
```

Unchecked Array Index\Path 21:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2540>

Status New

| | Source | Destination |
|------|--------------------|--------------------|
| File | kbengine/mbedtls.c | kbengine/mbedtls.c |
| Line | 552 | 552 |

| | | |
|--------|-----------|-----------|
| Object | sockindex | sockindex |
|--------|-----------|-----------|

Code Snippet

File Name kbengine/mbedtls.c
Method mbed_connect_step2(struct connectdata *conn,

```
....  
552.     conn->recv[sockindex] = mbed_recv;
```

Unchecked Array Index\Path 22:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2541>
Status New

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/mbedtls.c | kbengine/mbedtls.c |
| Line | 553 | 553 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/mbedtls.c
Method mbed_connect_step2(struct connectdata *conn,

```
....  
553.     conn->send[sockindex] = mbed_send;
```

Unchecked Array Index\Path 23:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2542>
Status New

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/mbedtls.c | kbengine/mbedtls.c |
| Line | 971 | 971 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/mbedtls.c
Method mbed_connect_common(struct connectdata *conn,

```
....  
971.         conn->recv[sockindex] = mbed_recv;
```

Unchecked Array Index\Path 24:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2543 |
| Status | New |

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/mbedtls.c | kbengine/mbedtls.c |
| Line | 972 | 972 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/mbedtls.c
Method mbed_connect_common(struct connectdata *conn,

```
....  
972.         conn->send[sockindex] = mbed_send;
```

Unchecked Array Index\Path 25:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2544 |
| Status | New |

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 838 | 838 |
| Object | s | s |

Code Snippet

File Name kbengine/multi.c
Method static int waitconnect_getsock(struct connectdata *conn,

```
....  
838.         sock[s] = conn->tempsock[i];
```

Unchecked Array Index\Path 26:

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

| | |
|--------|--|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2545 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 1506 | 1506 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/nss.c

Method static void Curl_nss_close(struct connectdata *conn, int sockindex)

```
....  
1506.      conn->sock[sockindex] = CURL_SOCKET_BAD;
```

Unchecked Array Index\Path 27:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2546>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 2180 | 2180 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/nss.c

Method static CURLcode nss_connect_common(struct connectdata *conn, int sockindex,

```
....  
2180.      conn->recv[sockindex] = nss_recv;
```

Unchecked Array Index\Path 28:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2547>

Status New

| | Source | Destination |
|------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 2181 | 2181 |

| | | |
|--------|-----------|-----------|
| Object | sockindex | sockindex |
|--------|-----------|-----------|

Code Snippet

File Name kbengine/nss.c

Method static CURLcode nss_connect_common(struct connectdata *conn, int sockindex,

```
....  
2181.     conn->send[sockindex] = nss_send;
```

Unchecked Array Index\Path 29:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2548>

Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 437 | 437 |
| Object | cur | cur |

Code Snippet

File Name kbengine/polarssl.c

Method polarssl_connect_step1(struct connectdata *conn,

```
....  
437.     protocols[cur] = NULL;
```

Unchecked Array Index\Path 30:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2549>

Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 468 | 468 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/polarssl.c

Method polarssl_connect_step2(struct connectdata *conn,

```
....  
468.      conn->recv[sockindex] = polarssl_recv;
```

Unchecked Array Index\Path 31:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2550 |
| Status | New |

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 469 | 469 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/polarssl.c
Method polarssl_connect_step2(struct connectdata *conn,

```
....  
469.      conn->send[sockindex] = polarssl_send;
```

Unchecked Array Index\Path 32:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2551 |
| Status | New |

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 828 | 828 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/polarssl.c
Method polarssl_connect_common(struct connectdata *conn,

```
....  
828.      conn->recv[sockindex] = polarssl_recv;
```

Unchecked Array Index\Path 33:

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

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2552](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2552)

Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 829 | 829 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/polarssl.c

Method polarssl_connect_common(struct connectdata *conn,

```
....  
829.         conn->send[sockindex] = polarssl_send;
```

Unchecked Array Index\Path 34:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2553>

Status New

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/RecastRegion.cpp | kbengine/RecastRegion.cpp |
| Line | 266 | 266 |
| Object | i | i |

Code Snippet

File Name kbengine/RecastRegion.cpp

Method static bool floodRegion(int x, int y, int i,

```
....  
266.         srcReg[i] = r;
```

Unchecked Array Index\Path 35:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2554>

Status New

| | Source | Destination |
|------|---------------------------|---------------------------|
| File | kbengine/RecastRegion.cpp | kbengine/RecastRegion.cpp |
| Line | 267 | 267 |

| | | |
|--------|---|---|
| Object | i | i |
|--------|---|---|

Code Snippet

File Name kbengine/RecastRegion.cpp
Method static bool floodRegion(int x, int y, int i,

```
....  
267.         srcDist[i] = 0;
```

Unchecked Array Index\Path 36:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2555>
Status New

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/RecastRegion.cpp | kbengine/RecastRegion.cpp |
| Line | 324 | 324 |
| Object | ci | ci |

Code Snippet

File Name kbengine/RecastRegion.cpp
Method static bool floodRegion(int x, int y, int i,

```
....  
324.         srcReg[ci] = 0;
```

Unchecked Array Index\Path 37:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2556>
Status New

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/RecastRegion.cpp | kbengine/RecastRegion.cpp |
| Line | 453 | 453 |
| Object | idx | idx |

Code Snippet

File Name kbengine/RecastRegion.cpp
Method static void expandRegions(int maxIter, unsigned short level,


```
.....
453.                srcReg[idx] = dirtyEntries[i].region;
```

Unchecked Array Index\Path 38:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2557 |
| Status | New |

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/RecastRegion.cpp | kbengine/RecastRegion.cpp |
| Line | 454 | 454 |
| Object | idx | idx |

Code Snippet

File Name kbengine/RecastRegion.cpp
Method static void expandRegions(int maxIter, unsigned short level,

```
.....
454.                srcDist[idx] = dirtyEntries[i].distance2;
```

Unchecked Array Index\Path 39:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2558 |
| Status | New |

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 222 | 222 |
| Object | n | n |

Code Snippet

File Name kbengine/schannel.c
Method get_alg_id_by_name(char *name)

```
.....
222.    tmp[n] = 0;
```

Unchecked Array Index\Path 40:

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

| | |
|--------|--|
| | BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2559 |
| Status | New |

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 1317 | 1317 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/schannel.c

Method schannel_connect_common(struct connectdata *conn, int sockindex,

```
....  
1317.      conn->recv[sockindex] = schannel_recv;
```

Unchecked Array Index\Path 41:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2560>

Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 1318 | 1318 |
| Object | sockindex | sockindex |

Code Snippet

File Name kbengine/schannel.c

Method schannel_connect_common(struct connectdata *conn, int sockindex,

```
....  
1318.      conn->send[sockindex] = schannel_send;
```

Unchecked Array Index\Path 42:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2561>

Status New

| | Source | Destination |
|------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 207 | 207 |

| | | |
|--------|-----|-----|
| Object | len | len |
|--------|-----|-----|

Code Snippet

File Name kbengine/sds.c

Method void sdsIncrLen(sds s, int incr) {

```
....  
207.      s[sh->len] = '\0';
```

Unchecked Array Index\Path 43:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2562>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 524 | 524 |
| Object | i | i |

Code Snippet

File Name kbengine/sds.c

Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....  
524.      s[i] = '\0';
```

Unchecked Array Index\Path 44:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2563>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 554 | 554 |
| Object | len | len |

Code Snippet

File Name kbengine/sds.c

Method void sdstrim(sds s, const char *cset) {

```
....  
554.      sh->buf[len] = '\0';
```

Unchecked Array Index\Path 45:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2564 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/smtp.c | kbengine/smtp.c |
| Line | 862 | 862 |
| Object | len | len |

Code Snippet

File Name kbengine/smtp.c
Method static CURLcode smtp_state_command_resp(struct connectdata *conn, int smtpcode,

```
....  
862.      line[len] = '\n';
```

Unchecked Array Index\Path 46:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2565 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/smtp.c | kbengine/smtp.c |
| Line | 864 | 864 |
| Object | len | len |

Code Snippet

File Name kbengine/smtp.c
Method static CURLcode smtp_state_command_resp(struct connectdata *conn, int smtpcode,

```
....  
864.      line[len] = '\0';
```

Unchecked Array Index\Path 47:

| | |
|----------|-----|
| Severity | Low |
|----------|-----|

| | |
|----------------|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2566 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/t1_enc.c | kbengine/t1_enc.c |
| Line | 1246 | 1246 |
| Object | currentvalpos | currentvalpos |

Code Snippet

File Name kbengine/t1_enc.c

Method int tls1_export_keying_material(SSL *s, unsigned char *out, size_t olen,

```
....  
1246.          val[currentvalpos] = (contextlen >> 8) & 0xff;
```

Unchecked Array Index\Path 48:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2567 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/t1_enc.c | kbengine/t1_enc.c |
| Line | 1248 | 1248 |
| Object | currentvalpos | currentvalpos |

Code Snippet

File Name kbengine/t1_enc.c

Method int tls1_export_keying_material(SSL *s, unsigned char *out, size_t olen,

```
....  
1248.          val[currentvalpos] = contextlen & 0xff;
```

Unchecked Array Index\Path 49:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2568 |
| Status | New |

| | Source | Destination |
|------|-------------------|-------------------|
| File | kbengine/telnet.c | kbengine/telnet.c |

| | | |
|--------|-----------------|-----------------|
| Line | 258 | 258 |
| Object | CURL_TELOPT_SGA | CURL_TELOPT_SGA |

Code Snippet

File Name kbengine/telnet.c

Method CURLcode init_telnet(struct connectdata *conn)

```
....
258.     tn->us_preferred[CURL_TELOPT_SGA] = CURL_YES;
```

Unchecked Array Index\Path 50:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2569>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/telnet.c | kbengine/telnet.c |
| Line | 259 | 259 |
| Object | CURL_TELOPT_SGA | CURL_TELOPT_SGA |

Code Snippet

File Name kbengine/telnet.c

Method CURLcode init_telnet(struct connectdata *conn)

```
....
259.     tn->him_preferred[CURL_TELOPT_SGA] = CURL_YES;
```

Sizeof Pointer Argument

Query Path:

CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

[Description](#)

Sizeof Pointer Argument\Path 1:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2440>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 267 | 267 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....  
267.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 2:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2441>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 267 | 267 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....  
267.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 3:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2442>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 303 | 303 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....  
303.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 4:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2443 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 267 | 303 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....  
267.     for(i = 0; i < NUM_OF_CIPHERS; i++) {  
....  
303.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 5:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2444 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 284 | 303 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....  
284.     for(i = 0; i<NUM_OF_CIPHERS; i++) {  
....  
303.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 6:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2445 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 303 | 303 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....  
303.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 7:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2446>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 267 | 303 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....  
267.     for(i = 0; i < NUM_OF_CIPHERS; i++) {  
....  
303.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 8:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2447>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 284 | 303 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....  
284.     for(i = 0; i<NUM_OF_CIPHERS; i++) {  
....  
303.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 9:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2448>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_cbc.c | kbengine/s3_cbc.c |
| Line | 681 | 681 |
| Object | mac_out | sizeof |

Code Snippet

File Name kbengine/s3_cbc.c

Method int ssl3_cbc_digest_record(const EVP_MD_CTX *ctx,

```
....  
681.     memset(mac_out, 0, sizeof(mac_out));
```

Sizeof Pointer Argument\Path 10:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2449>

Status New

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/evp_enc.c | kbengine/evp_enc.c |
| Line | 455 | 455 |
| Object | final | sizeof |

Code Snippet

File Name kbengine/evp_enc.c

Method int EVP_DecryptUpdate(EVP_CIPHER_CTX *ctx, unsigned char *out, int *outl,

```
.....
455.      OPENSSL_assert(b <= sizeof ctx->final);
```

Sizeof Pointer Argument\Path 11:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2450 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 284 | 284 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
.....
284.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 12:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2451 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 267 | 284 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
.....
267.      for(i = 0; i < NUM_OF_CIPHERS; i++) {
.....
284.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 13:

| | |
|----------|-----|
| Severity | Low |
|----------|-----|

| | |
|----------------|---|
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2452 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 284 | 284 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....  
284.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 14:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2453 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 267 | 284 |
| Object | cipherlist | sizeof |

Code Snippet

File Name kbengine/nss.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....  
267.      for(i = 0; i < NUM_OF_CIPHERS; i++) {  
....  
284.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 15:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2454 |
| Status | New |

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

| | | |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 820 | 820 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
```

Sizeof Pointer Argument\Path 16:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2455>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 821 | 820 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....
821.                ((sizeof(APR_OFF_T_FMT) == 4 &&
....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
```

Sizeof Pointer Argument\Path 17:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2456>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 824 | 820 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....
824.                (sizeof(APR_OFF_T_FMT) == 3 &&
.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
```

Sizeof Pointer Argument\Path 18:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2457>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 826 | 820 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....
826.                (sizeof(APR_OFF_T_FMT) > 4 &&
.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
```

Sizeof Pointer Argument\Path 19:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2458>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 831 | 820 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....
831.                fmt += (sizeof(APR_OFF_T_FMT) - 2);
.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
```

Sizeof Pointer Argument\Path 20:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2459 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 820 | 820 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
```

Sizeof Pointer Argument\Path 21:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2460 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 833 | 820 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```

.....
833.                else if ((sizeof(APR_INT64_T_FMT) == 4 &&
.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&

```

Sizeof Pointer Argument\Path 22:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2461 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 836 | 820 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```

.....
836.                (sizeof(APR_INT64_T_FMT) == 3 &&
.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&

```

Sizeof Pointer Argument\Path 23:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2462 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 838 | 820 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),


```
.....
838.                (sizeof(APR_INT64_T_FMT) > 4 &&
.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
```

Sizeof Pointer Argument\Path 24:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2463 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 843 | 820 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....
843.                fmt += (sizeof(APR_INT64_T_FMT) - 2);
.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
```

Sizeof Pointer Argument\Path 25:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2464 |
| Status | New |

| | Source | Destination |
|--------|---------------------------|---------------------------|
| File | kbengine/crypt_blowfish.c | kbengine/crypt_blowfish.c |
| Line | 863 | 863 |
| Object | ai | sizeof |

Code Snippet

File Name kbengine/crypt_blowfish.c
Method char *_crypt_blowfish_rn(const char *key, const char *setting,

```
.....
863.                !memcmp(ai, yi, sizeof(ai));
```

Sizeof Pointer Argument\Path 26:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2465 |
| Status | New |

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/evp_enc.c | kbengine/evp_enc.c |
| Line | 521 | 521 |
| Object | final | sizeof |

Code Snippet

File Name kbengine/evp_enc.c

Method int EVP_DecryptFinal_ex(EVP_CIPHER_CTX *ctx, unsigned char *out, int *outl)

```
....  
521.          OPENSSL_assert(b <= sizeof ctx->final);
```

Sizeof Pointer Argument\Path 27:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2466 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_cbc.c | kbengine/s3_cbc.c |
| Line | 625 | 625 |
| Object | hmac_pad | sizeof |

Code Snippet

File Name kbengine/s3_cbc.c

Method int ssl3_cbc_digest_record(const EVP_MD_CTX *ctx,

```
....  
625.          OPENSSL_assert(mac_secret_length <= sizeof(hmac_pad));
```

Sizeof Pointer Argument\Path 28:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2467 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 826 | 826 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....  
826.                (sizeof(APR_OFF_T_FMT) > 4 &&
```

Sizeof Pointer Argument\Path 29:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2468>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 820 | 826 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....  
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))  
&&  
....  
826.                (sizeof(APR_OFF_T_FMT) > 4 &&
```

Sizeof Pointer Argument\Path 30:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2469>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 821 | 826 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....  
821.                ((sizeof(APR_OFF_T_FMT) == 4 &&  
....  
826.                (sizeof(APR_OFF_T_FMT) > 4 &&
```

Sizeof Pointer Argument\Path 31:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2470>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 824 | 826 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....  
824.                (sizeof(APR_OFF_T_FMT) == 3 &&  
....  
826.                (sizeof(APR_OFF_T_FMT) > 4 &&
```

Sizeof Pointer Argument\Path 32:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2471>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 831 | 826 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....
831.                fmt += (sizeof(APR_OFF_T_FMT) - 2);
.....
826.                (sizeof(APR_OFF_T_FMT) > 4 &&
```

Sizeof Pointer Argument\Path 33:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2472 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 831 | 831 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....
831.                fmt += (sizeof(APR_OFF_T_FMT) - 2);
```

Sizeof Pointer Argument\Path 34:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2473 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 820 | 831 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
.....
831.                fmt += (sizeof(APR_OFF_T_FMT) - 2);
```

Sizeof Pointer Argument\Path 35:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2474 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 821 | 831 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....  
821.                ((sizeof(APR_OFF_T_FMT) == 4 &&  
.....  
831.                fmt += (sizeof(APR_OFF_T_FMT) - 2);
```

Sizeof Pointer Argument\Path 36:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2475 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 824 | 831 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....  
824.                (sizeof(APR_OFF_T_FMT) == 3 &&  
.....  
831.                fmt += (sizeof(APR_OFF_T_FMT) - 2);
```

Sizeof Pointer Argument\Path 37:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2476 |

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

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 826 | 831 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....  
826.                (sizeof(APR_OFF_T_FMT) > 4 &&  
....  
831.                fmt += (sizeof(APR_OFF_T_FMT) - 2);
```

Sizeof Pointer Argument\Path 38:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2477>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 838 | 838 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....  
838.                (sizeof(APR_INT64_T_FMT) > 4 &&
```

Sizeof Pointer Argument\Path 39:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2478>

Status New

| | Source | Destination |
|------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 833 | 838 |

| | | |
|--------|-----------------|--------|
| Object | APR_INT64_T_FMT | sizeof |
|--------|-----------------|--------|

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```

.....
833.             else if ((sizeof(APR_INT64_T_FMT) == 4 &&
.....
838.             (sizeof(APR_INT64_T_FMT) > 4 &&

```

Sizeof Pointer Argument\Path 40:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2479>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 836 | 838 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```

.....
836.             (sizeof(APR_INT64_T_FMT) == 3 &&
.....
838.             (sizeof(APR_INT64_T_FMT) > 4 &&

```

Sizeof Pointer Argument\Path 41:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2480>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 820 | 838 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),


```
.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
.....
838.                (sizeof(APR_INT64_T_FMT) > 4 &&
```

Sizeof Pointer Argument\Path 42:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2481 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 843 | 838 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
.....
843.                fmt += (sizeof(APR_INT64_T_FMT) - 2);
.....
838.                (sizeof(APR_INT64_T_FMT) > 4 &&
```

Sizeof Pointer Argument\Path 43:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2482 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/t1_enc.c | kbengine/t1_enc.c |
| Line | 1084 | 1084 |
| Object | header | sizeof |

Code Snippet

File Name kbengine/t1_enc.c
Method int tls1_mac(SSL *ssl, unsigned char *md, int send)

```
.....
1084.                if (EVP_DigestSignUpdate(mac_ctx, header, sizeof(header))
<= 0
```

Sizeof Pointer Argument\Path 44:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2483 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 824 | 824 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....  
824.                (sizeof(APR_OFF_T_FMT) == 3 &&
```

Sizeof Pointer Argument\Path 45:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2484 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 826 | 824 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....  
826.                (sizeof(APR_OFF_T_FMT) > 4 &&  
....  
824.                (sizeof(APR_OFF_T_FMT) == 3 &&
```

Sizeof Pointer Argument\Path 46:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2485 |

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

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 820 | 824 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```

.....
820.                if ((sizeof(APR_OFF_T_FMT) > sizeof(APR_INT64_T_FMT))
&&
.....
824.                (sizeof(APR_OFF_T_FMT) == 3 &&

```

Sizeof Pointer Argument\Path 47:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2486>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 821 | 824 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```

.....
821.                ((sizeof(APR_OFF_T_FMT) == 4 &&
.....
824.                (sizeof(APR_OFF_T_FMT) == 3 &&

```

Sizeof Pointer Argument\Path 48:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2487>

Status New

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

| | | |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 831 | 824 |
| Object | APR_OFF_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....  
831.                fmt += (sizeof(APR_OFF_T_FMT) - 2);  
....  
824.                (sizeof(APR_OFF_T_FMT) == 3 &&
```

Sizeof Pointer Argument\Path 49:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2488>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 836 | 836 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....  
836.                (sizeof(APR_INT64_T_FMT) == 3 &&
```

Sizeof Pointer Argument\Path 50:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2489>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 838 | 836 |
| Object | APR_INT64_T_FMT | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c
 Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```

.....
838.                (sizeof(APR_INT64_T_FMT) > 4 &&
.....
836.                (sizeof(APR_INT64_T_FMT) == 3 &&
  
```

Unchecked Return Value

Query Path:

CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

NIST SP 800-53: SI-11 Error Handling (P2)

Description

Unchecked Return Value\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2157 |
| Status | New |

The EXPORT method calls the strtok function, at line 120 of kbengine/_ctypes_test.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/_ctypes_test.c | kbengine/_ctypes_test.c |
| Line | 122 | 122 |
| Object | strtok | strtok |

Code Snippet

File Name kbengine/_ctypes_test.c
 Method EXPORT(char *)my_strtok(char *token, const char *delim)

```

.....
122.        return strtok(token, delim);
  
```

Unchecked Return Value\Path 2:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2158 |
| Status | New |

The Curl_axtls_version method calls the snprintf function, at line 681 of kbengine/axtls.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/axtls.c | kbengine/axtls.c |
| Line | 683 | 683 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/axtls.c

Method static size_t Curl_axtls_version(char *buffer, size_t size)

```
....  
683.     return snprintf(buffer, size, "axTLS/%s", ssl_version());
```

Unchecked Return Value\Path 3:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2159>

Status New

The Curl_getaddressinfo method calls the snprintf function, at line 622 of kbengine/connect.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/connect.c | kbengine/connect.c |
| Line | 658 | 658 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/connect.c

Method bool Curl_getaddressinfo(struct sockaddr *sa, char *addr,

```
....  
658.     snprintf(addr, MAX_IPADDR_LEN, "%s", su->sun_path);
```

Unchecked Return Value\Path 4:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2160>

Status New

The Curl_cyssl_version method calls the snprintf function, at line 777 of kbengine/cyssl.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cyassl.c | kbengine/cyassl.c |
| Line | 780 | 780 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/cyassl.c

Method static size_t Curl_cyassl_version(char *buffer, size_t size)

```
....  
780.     return snprintf(buffer, size, "wolfSSL/%s",  
wolfSSL_lib_version());
```

Unchecked Return Value\Path 5:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2161>

Status New

The dtls1_connect method calls the snprintf function, at line 164 of kbengine/d1_clnt.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_clnt.c | kbengine/d1_clnt.c |
| Line | 366 | 366 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/d1_clnt.c

Method int dtls1_connect(SSL *s)

```
....  
366.                                     snprintf((char *)labelbuffer,
```

Unchecked Return Value\Path 6:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2162>

Status New

The dtls1_connect method calls the snprintf function, at line 164 of kbengine/d1_clnt.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_clnt.c | kbengine/d1_clnt.c |
| Line | 509 | 509 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/d1_clnt.c
Method int dtls1_connect(SSL *s)

```
....  
509.             snprintf((char *)labelbuffer,  
sizeof(DTLS1_SCTP_AUTH_LABEL),
```

Unchecked Return Value\Path 7:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2163 |
| Status | New |

The dtls1_accept method calls the snprintf function, at line 162 of kbengine/d1_srvr.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_srvr.c | kbengine/d1_srvr.c |
| Line | 436 | 436 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/d1_srvr.c
Method int dtls1_accept(SSL *s)

```
....  
436.             snprintf((char *)labelbuffer,  
sizeof(DTLS1_SCTP_AUTH_LABEL),
```

Unchecked Return Value\Path 8:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2164 |
| Status | New |

The dtls1_accept method calls the snprintf function, at line 162 of kbengine/d1_srvr.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/d1_srvr.c | kbengine/d1_srvr.c |
| Line | 654 | 654 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/d1_srvr.c
Method int dtls1_accept(SSL *s)

```
....  
654.             snprintf((char *)labelbuffer,  
sizeof(DTLS1_SCTP_AUTH_LABEL),
```

Unchecked Return Value\Path 9:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2165 |
| Status | New |

The `*curl_easy_escape` method calls the `snprintf` function, at line 79 of `kbengine/escape.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/escape.c | kbengine/escape.c |
| Line | 125 | 125 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/escape.c
Method char *curl_easy_escape(struct Curl_easy *data, const char *string,

```
....  
125.             snprintf(&ns[strindex], 4, "%%02X", in);
```

Unchecked Return Value\Path 10:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2166 |
| Status | New |

The `ftp_state_use_port` method calls the `snprintf` function, at line 928 of `kbengine/ftp.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 1275 | 1275 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/ftp.c

Method static CURLcode ftp_state_use_port(struct connectdata *conn,

```
....
1275.         snprintf(dest, 20, "%d,%d", (int) (port>>8),
(int) (port&0xff));
```

Unchecked Return Value\Path 11:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2167>

Status New

The ftp_state_mdtm_resp method calls the snprintf function, at line 2043 of kbengine/ftp.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 2063 | 2063 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/ftp.c

Method static CURLcode ftp_state_mdtm_resp(struct connectdata *conn,

```
....
2063.         snprintf(timebuf, sizeof(timebuf),
```

Unchecked Return Value\Path 12:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2168>

Status New

The ftp_state_mdtm_resp method calls the snprintf function, at line 2043 of kbengine/ftp.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/ftp.c | kbengine/ftp.c |
| Line | 2088 | 2088 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/ftp.c

Method static CURLcode ftp_state_mdtm_resp(struct connectdata *conn,

```
....  
2088.          snprintf(headerbuf, sizeof(headerbuf),
```

Unchecked Return Value\Path 13:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2169>

Status New

The showtime method calls the snprintf function, at line 215 of kbengine/gtls.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |
| Line | 226 | 226 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/gtls.c

Method static void showtime(struct Curl_easy *data,

```
....  
226.          snprintf(str,
```

Unchecked Return Value\Path 14:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2170>

Status New

The Curl_gtls_version method calls the snprintf function, at line 1700 of kbengine/gtls.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

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

| | | |
|--------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |
| Line | 1702 | 1702 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/gtls.c

Method static size_t Curl_gtls_version(char *buffer, size_t size)

```
....  
1702.     return snprintf(buffer, size, "GnuTLS/%s",  
gnutls_check_version(NULL));
```

Unchecked Return Value\Path 15:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2171>

Status New

The *Curl_add_buffer_init method calls the calloc function, at line 1089 of kbengine/http.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 1091 | 1091 |
| Object | calloc | calloc |

Code Snippet

File Name kbengine/http.c

Method Curl_send_buffer *Curl_add_buffer_init(void)

```
....  
1091.     return calloc(1, sizeof(Curl_send_buffer));
```

Unchecked Return Value\Path 16:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2172>

Status New

The add_haproxy_protocol_header method calls the snprintf function, at line 1459 of kbengine/http.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

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

| | | |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 1474 | 1474 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/http.c

Method static CURLcode add_haproxy_protocol_header(struct connectdata *conn)

```
....  
1474.     snprintf(proxy_header,
```

Unchecked Return Value\Path 17:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2173>

Status New

The Curl_add_timecondition method calls the snprintf function, at line 1803 of kbengine/http.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |
| Line | 1846 | 1846 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/http.c

Method CURLcode Curl_add_timecondition(struct Curl_easy *data,

```
....  
1846.     snprintf(datestr, sizeof(datestr),
```

Unchecked Return Value\Path 18:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2174>

Status New

The Curl_http method calls the snprintf function, at line 1867 of kbengine/http.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|------|-----------------|-----------------|
| File | kbengine/http.c | kbengine/http.c |

| | | |
|--------|----------|----------|
| Line | 2276 | 2276 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/http.c

Method CURLcode Curl_http(struct connectdata *conn, bool *done)

```
....
2276.             snprintf(p, sizeof(ftp_typecode) - 1, ";type=%c",
```

Unchecked Return Value\Path 19:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2175>

Status New

The Curl_http2_ver method calls the snprintf function, at line 321 of kbengine/http2.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http2.c | kbengine/http2.c |
| Line | 324 | 324 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/http2.c

Method int Curl_http2_ver(char *p, size_t len)

```
....
324.     return snprintf(p, len, " nghttp2/%s", h2->version_str);
```

Unchecked Return Value\Path 20:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2176>

Status New

The imap_sendf method calls the snprintf function, at line 1727 of kbengine/imap.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |

| | | |
|--------|----------|----------|
| Line | 1740 | 1740 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/imap.c

Method static CURLcode imap_sendf(struct connectdata *conn, const char *fmt, ...)

```
....  
1740.     snprintf(imapc->resptag, sizeof(imapc->resptag), "%c%03d",
```

Unchecked Return Value\Path 21:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2177>

Status New

The *imap_atom method calls the strdup function, at line 1768 of kbengine/imap.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/imap.c | kbengine/imap.c |
| Line | 1807 | 1807 |
| Object | strdup | strdup |

Code Snippet

File Name kbengine/imap.c

Method static char *imap_atom(const char *str, bool escape_only)

```
....  
1807.     return strdup(str);
```

Unchecked Return Value\Path 22:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2178>

Status New

The Curl_mbedtls_version method calls the snprintf function, at line 815 of kbengine/mbedtls.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|------|--------------------|--------------------|
| File | kbengine/mbedtls.c | kbengine/mbedtls.c |

| | | |
|--------|----------|----------|
| Line | 818 | 818 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/mbedtls.c

Method static size_t Curl_mbedtls_version(char *buffer, size_t size)

```
....  
818.     return snprintf(buffer, size, "mbedtls/%u.%u.%u", version>>24,
```

Unchecked Return Value\Path 23:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2179>

Status New

The *curl_maprintf method calls the strdup function, at line 1066 of kbengine/mprintf.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/mprintf.c | kbengine/mprintf.c |
| Line | 1089 | 1089 |
| Object | strdup | strdup |

Code Snippet

File Name kbengine/mprintf.c

Method char *curl_maprintf(const char *format, ...)

```
....  
1089.     return strdup("");
```

Unchecked Return Value\Path 24:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2180>

Status New

The *curl_mvaprintf method calls the strdup function, at line 1092 of kbengine/mprintf.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|------|--------------------|--------------------|
| File | kbengine/mprintf.c | kbengine/mprintf.c |

| | | |
|--------|--------|--------|
| Line | 1113 | 1113 |
| Object | strdup | strdup |

Code Snippet

File Name kbengine/mprintf.c

Method char *curl_mvaprintf(const char *format, va_list ap_save)

```
....
1113.     return strdup("");
```

Unchecked Return Value\Path 25:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2181>

Status New

The multi_done method calls the snprintf function, at line 515 of kbengine/multi.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/multi.c | kbengine/multi.c |
| Line | 636 | 636 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/multi.c

Method static CURLcode multi_done(struct connectdata **connp,

```
....
636.     snprintf(buffer, sizeof(buffer),
```

Unchecked Return Value\Path 26:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2182>

Status New

The *dup_nickname method calls the strdup function, at line 361 of kbengine/nss.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 367 | 367 |

| | | |
|--------|--------|--------|
| Object | strdup | strdup |
|--------|--------|--------|

Code Snippet

File Name kbengine/nss.c

Method static char *dup_nickname(struct Curl_easy *data, const char *str)

```
....  
367.         return strdup(str);
```

Unchecked Return Value\Path 27:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2183>

Status New

The *dup_nickname method calls the strdup function, at line 361 of kbengine/nss.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 374 | 374 |
| Object | strdup | strdup |

Code Snippet

File Name kbengine/nss.c

Method static char *dup_nickname(struct Curl_easy *data, const char *str)

```
....  
374.         return strdup(str);
```

Unchecked Return Value\Path 28:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2184>

Status New

The Curl_nss_version method calls the sprintf function, at line 2277 of kbengine/nss.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 2279 | 2279 |

| | | |
|--------|----------|----------|
| Object | snprintf | snprintf |
|--------|----------|----------|

Code Snippet

File Name kbengine/nss.c

Method static size_t Curl_nss_version(char *buffer, size_t size)

```
....  
2279.     return snprintf(buffer, size, "NSS/%s", NSS_VERSION);
```

Unchecked Return Value\Path 29:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2185>

Status New

The Curl_polarssl_version method calls the snprintf function, at line 719 of kbengine/polarssl.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 722 | 722 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/polarssl.c

Method static size_t Curl_polarssl_version(char *buffer, size_t size)

```
....  
722.     return snprintf(buffer, size, "%s/%d.%d.%d",
```

Unchecked Return Value\Path 30:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2186>

Status New

The pop3_perform_apop method calls the snprintf function, at line 413 of kbengine/pop3.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|------|-----------------|-----------------|
| File | kbengine/pop3.c | kbengine/pop3.c |
| Line | 446 | 446 |

| | | |
|--------|----------|----------|
| Object | snprintf | snprintf |
|--------|----------|----------|

Code Snippet

File Name kbengine/pop3.c

Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
446.      snprintf(&secret[2 * i], 3, "%02x", digest[i]);
```

Unchecked Return Value\Path 31:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2187>

Status New

The schannel_connect_step2 method calls the malloc function, at line 823 of kbengine/schannel.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/schannel.c | kbengine/schannel.c |
| Line | 925 | 925 |
| Object | malloc | malloc |

Code Snippet

File Name kbengine/schannel.c

Method schannel_connect_step2(struct connectdata *conn, int sockindex)

```
....
925.      InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc (BACKEND-
>encdata_offset),
```

Unchecked Return Value\Path 32:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2188>

Status New

The myssh_statemach_act method calls the snprintf function, at line 546 of kbengine/ssh-libssh.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|------|-----------------------|-----------------------|
| File | kbengine/ssh-libssh.c | kbengine/ssh-libssh.c |
| Line | 1345 | 1345 |

| | | |
|--------|----------|----------|
| Object | snprintf | snprintf |
|--------|----------|----------|

Code Snippet

File Name kbengine/ssh-libssh.c

Method static CURLcode myssh_statemach_act(struct connectdata *conn, bool *block)

```
....
1345.             snprintf(sshc->readdir_linkPath, PATH_MAX, "%s%s",
protop->path,
```

Unchecked Return Value\Path 33:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2189>

Status New

The check_telnet_options method calls the snprintf function, at line 818 of kbengine/telnet.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/telnet.c | kbengine/telnet.c |
| Line | 832 | 832 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/telnet.c

Method static CURLcode check_telnet_options(struct connectdata *conn)

```
....
832.             snprintf(option_arg, sizeof(option_arg), "USER,%s", conn-
>user);
```

Unchecked Return Value\Path 34:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2190>

Status New

The suboption method calls the snprintf function, at line 922 of kbengine/telnet.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|------|-------------------|-------------------|
| File | kbengine/telnet.c | kbengine/telnet.c |
| Line | 938 | 938 |

| | | |
|--------|----------|----------|
| Object | snprintf | snprintf |
|--------|----------|----------|

Code Snippet

File Name kbengine/telnet.c

Method static void suboption(struct connectdata *conn)

```
....  
938.          snprintf((char *)temp, sizeof(temp),
```

Unchecked Return Value\Path 35:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2191>

Status New

The suboption method calls the snprintf function, at line 922 of kbengine/telnet.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/telnet.c | kbengine/telnet.c |
| Line | 950 | 950 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/telnet.c

Method static void suboption(struct connectdata *conn)

```
....  
950.          snprintf((char *)temp, sizeof(temp),
```

Unchecked Return Value\Path 36:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2192>

Status New

The suboption method calls the snprintf function, at line 922 of kbengine/telnet.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/telnet.c | kbengine/telnet.c |
| Line | 961 | 961 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/telnet.c

Method static void suboption(struct connectdata *conn)

```
....  
961.          snprintf((char *)temp, sizeof(temp),
```

Unchecked Return Value\Path 37:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2193>

Status New

The suboption method calls the snprintf function, at line 922 of kbengine/telnet.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/telnet.c | kbengine/telnet.c |
| Line | 971 | 971 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/telnet.c

Method static void suboption(struct connectdata *conn)

```
....  
971.          snprintf((char *)&temp[len], sizeof(temp) - len,
```

Unchecked Return Value\Path 38:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2194>

Status New

The suboption method calls the snprintf function, at line 922 of kbengine/telnet.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/telnet.c | kbengine/telnet.c |
| Line | 978 | 978 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/telnet.c

Method static void suboption(struct connectdata *conn)

```
....  
978.          snprintf((char *)&temp[len], sizeof(temp) - len,
```

Unchecked Return Value\Path 39:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2195 |
| Status | New |

The `flatten_match` method calls the `sprintf` function, at line 94 of `kbengine/testbuckets.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------------------------|-------------------------------------|
| File | <code>kbengine/testbuckets.c</code> | <code>kbengine/testbuckets.c</code> |
| Line | 103 | 103 |
| Object | <code>sprintf</code> | <code>sprintf</code> |

Code Snippet

File Name `kbengine/testbuckets.c`
Method `static void flatten_match(abts_case *tc, const char *ctx,`

```
....  
103.          sprintf(msg, "%s: flatten brigade", ctx);
```

Unchecked Return Value\Path 40:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2196 |
| Status | New |

The `flatten_match` method calls the `sprintf` function, at line 94 of `kbengine/testbuckets.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------------------------|-------------------------------------|
| File | <code>kbengine/testbuckets.c</code> | <code>kbengine/testbuckets.c</code> |
| Line | 105 | 105 |
| Object | <code>sprintf</code> | <code>sprintf</code> |

Code Snippet

File Name `kbengine/testbuckets.c`
Method `static void flatten_match(abts_case *tc, const char *ctx,`


```
....  
105.      sprintf(msg, "%s: length match (%ld not %ld)", ctx,
```

Unchecked Return Value\Path 41:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2197 |
| Status | New |

The `flatten_match` method calls the `sprintf` function, at line 94 of `kbengine/testbuckets.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------------------------|-------------------------------------|
| File | <code>kbengine/testbuckets.c</code> | <code>kbengine/testbuckets.c</code> |
| Line | 108 | 108 |
| Object | <code>sprintf</code> | <code>sprintf</code> |

Code Snippet

File Name `kbengine/testbuckets.c`
Method `static void flatten_match(abts_case *tc, const char *ctx,`

```
....  
108.      sprintf(msg, "%s: result match", msg);
```

Unchecked Return Value\Path 42:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2198 |
| Status | New |

The `test_splits` method calls the `strdup` function, at line 229 of `kbengine/testbuckets.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------------------------|-------------------------------------|
| File | <code>kbengine/testbuckets.c</code> | <code>kbengine/testbuckets.c</code> |
| Line | 244 | 244 |
| Object | <code>strdup</code> | <code>strdup</code> |

Code Snippet

File Name `kbengine/testbuckets.c`
Method `static void test_splits(abts_case *tc, void *ctx)`

```
.....
244.                                apr_bucket_heap_create(strdup(str), 9,
free, ba));
```

Unchecked Return Value\Path 43:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2199 |
| Status | New |

The `*parse_filename` method calls the `snprintf` function, at line 185 of `kbengine/tool_cb_hdr.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|------------------------|------------------------|
| File | kbengine/tool_cb_hdr.c | kbengine/tool_cb_hdr.c |
| Line | 267 | 267 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/tool_cb_hdr.c
Method static char *parse_filename(const char *ptr, size_t len)

```
.....
267.                                snprintf(buffer, sizeof(buffer), "%s/%s", tdir, copy);
```

Unchecked Return Value\Path 44:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2200 |
| Status | New |

The `get_url_file_name` method calls the `snprintf` function, at line 130 of `kbengine/tool_operhlp.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operhlp.c | kbengine/tool_operhlp.c |
| Line | 179 | 179 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/tool_operhlp.c
Method CURLcode get_url_file_name(char **filename, const char *url)

```
.....  
179.          snprintf(buffer, sizeof(buffer), "%s/%s", tdir, *filename);
```

Unchecked Return Value\Path 45:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2201 |
| Status | New |

The `parse_remote_port` method calls the `snprintf` function, at line 3345 of `kbengine/url.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-----------------------------|-----------------------------|
| File | <code>kbengine/url.c</code> | <code>kbengine/url.c</code> |
| Line | 3400 | 3400 |
| Object | <code>snprintf</code> | <code>snprintf</code> |

Code Snippet

File Name `kbengine/url.c`
Method `static CURLcode parse_remote_port(struct Curl_easy *data,`

```
.....  
3400.          snprintf(type, sizeof(type), ";type=%c",
```

Unchecked Return Value\Path 46:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2202 |
| Status | New |

The `*curl_version_info` method calls the `snprintf` function, at line 383 of `kbengine/version.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|---------------------------------|---------------------------------|
| File | <code>kbengine/version.c</code> | <code>kbengine/version.c</code> |
| Line | 439 | 439 |
| Object | <code>snprintf</code> | <code>snprintf</code> |

Code Snippet

File Name `kbengine/version.c`
Method `curl_version_info_data *curl_version_info(CURLversion stamp)`

```
....  
439.     snprintf(ssh_buffer, sizeof(ssh_buffer), "libssh2/%s",  
LIBSSH2_VERSION);
```

Unchecked Return Value\Path 47:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2203 |
| Status | New |

The `brotnli_version` method calls the `snprintf` function, at line 91 of `kbengine/version.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/version.c | kbengine/version.c |
| Line | 98 | 98 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/version.c
Method static size_t brotnli_version(char *buf, size_t bufsz)

```
....  
98.     return snprintf(buf, bufsz, "%u.%u.%u", major, minor, patch);
```

Unchecked Return Value\Path 48:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2204 |
| Status | New |

The `*curl_version` method calls the `snprintf` function, at line 102 of `kbengine/version.c`. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/version.c | kbengine/version.c |
| Line | 200 | 200 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/version.c
Method char *curl_version(void)

```
....
200.      snprintf(ptr, left, " librtmp/%d.%d%s",
```

Unchecked Return Value\Path 49:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2205 |
| Status | New |

The Curl_ssl_push_certinfo_len method calls the snprintf function, at line 685 of kbengine/vtls.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |
| Line | 703 | 703 |
| Object | snprintf | snprintf |

Code Snippet

File Name kbengine/vtls.c
Method CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
703.      snprintf(output, outlen, "%s:", label);
```

Unchecked Return Value\Path 50:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2206 |
| Status | New |

The strstore method calls the Pointer function, at line 368 of kbengine/cookie.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 371 | 371 |
| Object | Pointer | Pointer |

Code Snippet

File Name kbengine/cookie.c
Method static void strstore(char **str, const char *newstr)

```
....
371.      *str = strdup(newstr);
```

Use of Sizeof On a Pointer Type

Query Path:

CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

[Description](#)

Use of Sizeof On a Pointer Type\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2227 |
| Status | New |

| | Source | Destination |
|--------|----------------------------|----------------------------|
| File | kbengine/apr_dbd_freetds.c | kbengine/apr_dbd_freetds.c |
| Line | 403 | 403 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/apr_dbd_freetds.c

Method static int recurse_args(apr_pool_t *pool, int n, const char *query,

```
....
403.          stmt->taint = apr_palloc(pool, n*sizeof(regex_t*));
```

Use of Sizeof On a Pointer Type\Path 2:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2228 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/apr_snprintf.c | kbengine/apr_snprintf.c |
| Line | 1119 | 1119 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/apr_snprintf.c

Method APR_DECLARE(int) apr_vformatter(int (*flush_func)(apr_vformatter_buff_t *),

```
....
1119.          if (sizeof(void *) <= sizeof(apr_uint64_t)) {
```

Use of Sizeof On a Pointer Type\Path 3:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2229 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1289 | 1289 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/cookie.c

Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....  
1289.      array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 4:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2230 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1299 | 1299 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/cookie.c

Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....  
1299.      qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 5:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2231 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1474 | 1474 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/cookie.c

Method static int cookie_output(struct CookieInfo *c, const char *dumphere)

```
....  
1474.    array = malloc(sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2232>

Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1505 | 1505 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/cookie.c

Method static int cookie_output(struct CookieInfo *c, const char *dumphere)

```
....  
1505.    qsort(array, c->numcookies, sizeof(struct Cookie *),  
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2233>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/easy.c | kbengine/easy.c |
| Line | 860 | 860 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/easy.c

Method static CURLcode dupset(struct Curl_easy *dst, struct Curl_easy *src)

```
....  
860.     memset(dst->set.str, 0, STRING_LAST * sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 8:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2234>

Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http2.c | kbengine/http2.c |
| Line | 926 | 926 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/http2.c

Method static int on_header(nghttp2_session *session, const nghttp2_frame *frame,

```
....  
926.                                     sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 9:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2235>

Status New

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/http2.c | kbengine/http2.c |
| Line | 934 | 934 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/http2.c

Method static int on_header(nghttp2_session *session, const nghttp2_frame *frame,

```
....  
934.                                     stream->push_headers_alloc *  
sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 10:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2236 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_enc.c | kbengine/s3_enc.c |
| Line | 609 | 609 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/s3_enc.c
Method int ssl3_digest_cached_records(SSL *s)

```
....  
609.          OPENSSL_malloc(SSL_MAX_DIGEST * sizeof(EVP_MD_CTX *));
```

Use of Sizeof On a Pointer Type\Path 11:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2237 |
| Status | New |

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/s3_enc.c | kbengine/s3_enc.c |
| Line | 610 | 610 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/s3_enc.c
Method int ssl3_digest_cached_records(SSL *s)

```
....  
610.          memset(s->s3->handshake_dgst, 0, SSL_MAX_DIGEST *  
sizeof(EVP_MD_CTX *));
```

Use of Sizeof On a Pointer Type\Path 12:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2238 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 905 | 905 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/sds.c

Method sds *sdssplitargs(const char *line, int *argc) {

```
....  
905.                vector = realloc(vector, ((*argc)+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 13:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2239>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/sds.c | kbengine/sds.c |
| Line | 911 | 911 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/sds.c

Method sds *sdssplitargs(const char *line, int *argc) {

```
....  
911.                if (vector == NULL) vector = malloc(sizeof(void*));
```

Use of Sizeof On a Pointer Type\Path 14:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2240>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |
| Line | 672 | 672 |
| Object | sizeof | sizeof |

Code Snippet

File Name kbengine/vtls.c
Method CURLcode Curl_ssl_init_certinfo(struct Curl_easy *data, int num)

```
....
672.     table = calloc((size_t) num, sizeof(struct curl_slist *));
```

Incorrect Permission Assignment For Critical Resources

Query Path:

CPP\Cx\CPP Low Visibility\Incorrect Permission Assignment For Critical Resources Version:1

Categories

FISMA 2014: Access Control

NIST SP 800-53: AC-3 Access Enforcement (P1)

OWASP Top 10 2017: A2-Broken Authentication

Description

Incorrect Permission Assignment For Critical Resources\Path 1:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2135>
Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/filestat.c | kbengine/filestat.c |
| Line | 136 | 136 |
| Object | chmod | chmod |

Code Snippet

File Name kbengine/filestat.c
Method APR_DECLARE(apr_status_t) apr_file_perms_set(const char *fname,

```
....
136.     if (chmod(fname, mode) == -1)
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2136>
Status New

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1484 | 1484 |
| Object | out | out |

Code Snippet

File Name kbengine/cookie.c

Method static int cookie_output(struct CookieInfo *c, const char *dumphere)

```
....  
1484.      out = fopen(dumphere, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2137>

Status New

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |
| Line | 248 | 248 |
| Object | f | f |

Code Snippet

File Name kbengine/gtls.c

Method static gnutls_datum_t load_file(const char *file)

```
....  
248.      f = fopen(file, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2138>

Status New

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 149 | 149 |
| Object | file | file |

Code Snippet

File Name kbengine/tool_operate.c

Method static curl_off_t vms_realfilesize(const char *name,

```
....  
149.      file = fopen(name, "r"); /* VMS */
```

Incorrect Permission Assignment For Critical Resources\Path 5:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2139 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |
| Line | 893 | 893 |
| Object | fp | fp |

Code Snippet

File Name kbengine/vtls.c

Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....  
893.      fp = fopen(pinnedpubkey, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2140 |
| Status | New |

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 345 | 345 |
| Object | newfile | newfile |

Code Snippet

File Name kbengine/tool_operate.c

Method static CURLcode operate_do(struct GlobalConfig *global,

```
....  
345.      FILE *newfile = fopen(config->headerfile, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2141 |
| Status | New |

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

| | | |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 623 | 623 |
| Object | file | file |

Code Snippet

File Name kbengine/tool_operate.c

Method static CURLcode operate_do(struct GlobalConfig *global,

```
....  
623.             FILE *file = fopen(outfile, config-  
>resume_from?"ab":"wb",
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2142>

Status New

| | Source | Destination |
|--------|----------------------------|----------------------------|
| File | kbengine/schannel_verify.c | kbengine/schannel_verify.c |
| Line | 111 | 111 |
| Object | CreateFile | CreateFile |

Code Snippet

File Name kbengine/schannel_verify.c

Method static CURLcode add_certs_to_store(HCERTSTORE trust_store,

```
....  
111.     ca_file_handle = CreateFile(ca_file_tstr,
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2143>

Status New

| | Source | Destination |
|--------|--------------------------|--------------------------|
| File | kbengine/tool_filetime.c | kbengine/tool_filetime.c |
| Line | 106 | 106 |
| Object | CreateFileA | CreateFileA |

Code Snippet

File Name kbengine/tool_filetime.c

Method void setfiletime(curl_off_t filetime, const char *filename,

```
....
106.      hfile = CreateFileA(filename, FILE_WRITE_ATTRIBUTES,
```

Incorrect Permission Assignment For Critical Resources\Path 10:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2144 |
| Status | New |

| | Source | Destination |
|--------|--------------------------|--------------------------|
| File | kbengine/tool_filetime.c | kbengine/tool_filetime.c |
| Line | 40 | 40 |
| Object | CreateFileA | CreateFileA |

Code Snippet

File Name kbengine/tool_filetime.c
Method curl_off_t getfiletime(const char *filename, FILE *error_stream)

```
....
40.      hfile = CreateFileA(filename, FILE_READ_ATTRIBUTES,
```

Potential Off by One Error in Loops

Query Path:

CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=417 |
| Status | New |

The buffer allocated by <= in kbengine/blast.c at line 191 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|------|------------------|------------------|
| File | kbengine/blast.c | kbengine/blast.c |
| Line | 212 | 212 |

| | | |
|--------|----|----|
| Object | <= | <= |
|--------|----|----|

Code Snippet

File Name kbengine/blast.c

Method local int construct(struct huffman *h, const unsigned char *rep, int n)

```
....
212.      for (len = 0; len <= MAXBITS; len++)
```

Potential Off by One Error in Loops\Path 2:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=418>

Status New

The buffer allocated by <= in kbengine/curl_path.c at line 113 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/curl_path.c | kbengine/curl_path.c |
| Line | 140 | 140 |
| Object | <= | <= |

Code Snippet

File Name kbengine/curl_path.c

Method CURLcode Curl_get_pathname(const char **cpp, char **path, char *homedir)

```
....
140.      for(i = j = 0; i <= strlen(cp); i++) {
```

Potential Off by One Error in Loops\Path 3:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=419>

Status New

The buffer allocated by <= in kbengine/e_aes.c at line 1031 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/e_aes.c | kbengine/e_aes.c |
| Line | 1041 | 1041 |
| Object | <= | <= |

Code Snippet

File Name kbengine/e_aes.c

Method static int aes_ecb_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
1041.         for (i = 0, len -= bl; i <= len; i += bl)
```

Potential Off by One Error in Loops\Path 4:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=420>

Status New

The buffer allocated by <= in kbengine/e_aes_cbc_hmac_sha1.c at line 207 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|--------|--------------------------------|--------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha1.c | kbengine/e_aes_cbc_hmac_sha1.c |
| Line | 428 | 428 |
| Object | <= | <= |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha1.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA1 *key,

```
....
428.         for (j = 0; j <= pad; j++)
```

Potential Off by One Error in Loops\Path 5:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=421>

Status New

The buffer allocated by <= in kbengine/e_aes_cbc_hmac_sha256.c at line 203 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/e_aes_cbc_hmac_sha256.c | kbengine/e_aes_cbc_hmac_sha256.c |
| Line | 443 | 443 |
| Object | <= | <= |

Code Snippet

File Name kbengine/e_aes_cbc_hmac_sha256.c

Method static size_t tls1_1_multi_block_encrypt(EVP_AES_HMAC_SHA256 *key,

```
.....
443.          for (j = 0; j <= pad; j++)
```

Potential Off by One Error in Loops\Path 6:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=422 |
| Status | New |

The buffer allocated by <= in kbengine/obj_dat.c at line 259 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/obj_dat.c | kbengine/obj_dat.c |
| Line | 287 | 287 |
| Object | <= | <= |

Code Snippet

File Name kbengine/obj_dat.c
Method int OBJ_add_object(const ASN1_OBJECT *obj)

```
.....
287.          for (i = ADDED_DATA; i <= ADDED_NID; i++) {
```

Potential Off by One Error in Loops\Path 7:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=423 |
| Status | New |

The buffer allocated by <= in kbengine/obj_dat.c at line 259 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/obj_dat.c | kbengine/obj_dat.c |
| Line | 305 | 305 |
| Object | <= | <= |

Code Snippet

File Name kbengine/obj_dat.c
Method int OBJ_add_object(const ASN1_OBJECT *obj)

```
....
305.         for (i = ADDED_DATA; i <= ADDED_NID; i++)
```

Potential Off by One Error in Loops\Path 8:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=424 |
| Status | New |

The buffer allocated by <= in kbengine/puff.c at line 340 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/puff.c | kbengine/puff.c |
| Line | 348 | 348 |
| Object | <= | <= |

Code Snippet

File Name kbengine/puff.c
Method local int construct(struct huffman *h, const short *length, int n)

```
....
348.         for (len = 0; len <= MAXBITS; len++)
```

Potential Off by One Error in Loops\Path 9:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=425 |
| Status | New |

The buffer allocated by <= in kbengine/RecastMeshDetail.cpp at line 638 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|--------|-------------------------------|-------------------------------|
| File | kbengine/RecastMeshDetail.cpp | kbengine/RecastMeshDetail.cpp |
| Line | 703 | 703 |
| Object | <= | <= |

Code Snippet

File Name kbengine/RecastMeshDetail.cpp
Method static bool buildPolyDetail(rcContext* ctx, const float* in, const int nin,

```
.....  
703.                for (int k = 0; k <= nn; ++k)
```

Information Exposure Through Comments

Query Path:

CPP\Cx\CPP Low Visibility\Information Exposure Through Comments Version:1

Categories

FISMA 2014: Identification And Authentication

NIST SP 800-53: SC-28 Protection of Information at Rest (P1)

Description

Information Exposure Through Comments\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2146 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/_ssl.c | kbengine/_ssl.c |
| Line | 1968 | 1968 |
| Object | cipher [| cipher [|

Code Snippet

File Name kbengine/_ssl.c
Method _ssl._SSLSocket.cipher

```
.....  
1968.  _ssl._SSLSocket.cipher
```

Information Exposure Through Comments\Path 2:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2147 |
| Status | New |

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/_ssl.c | kbengine/_ssl.c |
| Line | 3770 | 3770 |
| Object | password: | password: |

Code Snippet

File Name kbengine/_ssl.c

Method keyfile: object = NULL

```
....  
3770.      keyfile: object = NULL
```

Information Exposure Through Comments\Path 3:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2148>
Status New

| | Source | Destination |
|--------|----------------------|----------------------|
| File | kbengine/darwinssl.c | kbengine/darwinssl.c |
| Line | 847 | 847 |
| Object | cipher- | cipher- |

Code Snippet

File Name kbengine/darwinssl.c
Method /* New ChaCha20+Poly1305 cipher-suites used by TLS 1.3: */

```
....  
847.      /* New ChaCha20+Poly1305 cipher-suites used by TLS 1.3: */
```

Information Exposure Through Comments\Path 4:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2149>
Status New

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/evp_enc.c | kbengine/evp_enc.c |
| Line | 83 | 83 |
| Object | cipher= | cipher= |

Code Snippet

File Name kbengine/evp_enc.c
Method /* ctx->cipher=NULL; */

```
....  
83.      /* ctx->cipher=NULL; */
```

Information Exposure Through Comments\Path 5:

Severity Low
Result State To Verify

| | |
|----------------|---|
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2150 |
| Status | New |

| | Source | Destination |
|--------|------------------|------------------|
| File | kbengine/gskit.c | kbengine/gskit.c |
| Line | 828 | 828 |
| Object | password (C | password (C |

Code Snippet

File Name kbengine/gskit.c

Method * Key password (CURLOPT_KEYPASSWD) holds the keyring password.

```
....  
828.      * Key password (CURLOPT_KEYPASSWD) holds the keyring password.
```

Information Exposure Through Comments\Path 6:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2151 |
| Status | New |

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/nss.c | kbengine/nss.c |
| Line | 317 | 317 |
| Object | cipher- | cipher- |

Code Snippet

File Name kbengine/nss.c

Method * Return true if at least one cipher-suite is enabled. Used to determine

```
....  
317.      * Return true if at least one cipher-suite is enabled. Used to  
determine
```

Information Exposure Through Comments\Path 7:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2152 |
| Status | New |

| | Source | Destination |
|------|--------------------|--------------------|
| File | kbengine/ssltest.c | kbengine/ssltest.c |

| | | |
|--------|----------|----------|
| Line | 1238 | 1238 |
| Object | cipher = | cipher = |

Code Snippet

File Name kbengine/ssltest.c

Method /* if (cipher == NULL) cipher=getenv("SSL_CIPHER"); */

```
....  
1238. /* if (cipher == NULL) cipher=getenv("SSL_CIPHER"); */
```

Information Exposure Through Comments\Path 8:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2153>

Status New

| | Source | Destination |
|--------|--------------------|--------------------|
| File | kbengine/ssltest.c | kbengine/ssltest.c |
| Line | 1238 | 1238 |
| Object | cipher= | cipher= |

Code Snippet

File Name kbengine/ssltest.c

Method /* if (cipher == NULL) cipher=getenv("SSL_CIPHER"); */

```
....  
1238. /* if (cipher == NULL) cipher=getenv("SSL_CIPHER"); */
```

Information Exposure Through Comments\Path 9:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2154>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 3546 | 3546 |
| Object | password (o | password (o |

Code Snippet

File Name kbengine/url.c

Method /* Store the password (only if user is present), zero-length if not set */


```
.....
3546.      /* Store the password (only if user is present), zero-length
if not set */
```

TOCTOU

Query Path:

CPP\Cx\CPP Low Visibility\TOCTOU Version:1

[Description](#)

TOCTOU\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2610 |
| Status | New |

The *Curl_cookie_init method in kbengine/cookie.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1079 | 1079 |
| Object | fopen | fopen |

Code Snippet

File Name kbengine/cookie.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
.....
1079.      fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 2:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2611 |
| Status | New |

The cookie_output method in kbengine/cookie.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/cookie.c | kbengine/cookie.c |
| Line | 1484 | 1484 |
| Object | fopen | fopen |

Code Snippet

File Name kbengine/cookie.c
Method static int cookie_output(struct CookieInfo *c, const char *dumphere)

```
....  
1484.         out = fopen(dumphere, FOPEN_WRITETEXT);
```

TOCTOU\Path 3:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2612>
Status New

The load_file method in kbengine/gtls.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/gtls.c | kbengine/gtls.c |
| Line | 248 | 248 |
| Object | fopen | fopen |

Code Snippet

File Name kbengine/gtls.c
Method static gnutls_datum_t load_file(const char *file)

```
....  
248.         f = fopen(file, "rb");
```

TOCTOU\Path 4:

Severity Low
Result State To Verify
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2613>
Status New

The vms_realfilesize method in kbengine/tool_operate.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 149 | 149 |
| Object | fopen | fopen |

Code Snippet

File Name kbengine/tool_operate.c
Method static curl_off_t vms_realfilesize(const char *name,

```
....  
149.     file = fopen(name, "r"); /* VMS */
```

TOCTOU\Path 5:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2614 |
| Status | New |

The operate_do method in kbengine/tool_operate.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 345 | 345 |
| Object | fopen | fopen |

Code Snippet

File Name kbengine/tool_operate.c
Method static CURLcode operate_do(struct GlobalConfig *global,

```
....  
345.     FILE *newfile = fopen(config->headerfile, "wb");
```

TOCTOU\Path 6:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2615 |
| Status | New |

The operate_do method in kbengine/tool_operate.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 623 | 623 |
| Object | fopen | fopen |

Code Snippet

File Name kbengine/tool_operate.c
Method static CURLcode operate_do(struct GlobalConfig *global,

```
.....
623.             FILE *file = fopen(outfile, config-
>resume_from?"ab":"wb",
```

TOCTOU\Path 7:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2616 |
| Status | New |

The Curl_pin_peer_pubkey method in kbengine/vtls.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |
| Line | 893 | 893 |
| Object | fopen | fopen |

Code Snippet

File Name kbengine/vtls.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
.....
893.     fp = fopen(pinnedpubkey, "rb");
```

TOCTOU\Path 8:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2617 |
| Status | New |

The operate_do method in kbengine/tool_operate.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 679 | 679 |
| Object | open | open |

Code Snippet

File Name kbengine/tool_operate.c
Method static CURLcode operate_do(struct GlobalConfig *global,

```
....
679.          infd = open(uploadfile, O_RDONLY | O_BINARY);
```

TOCTOU\Path 9:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2618 |
| Status | New |

The operate_do method in kbengine/tool_operate.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

| | Source | Destination |
|--------|-------------------------|-------------------------|
| File | kbengine/tool_operate.c | kbengine/tool_operate.c |
| Line | 682 | 682 |
| Object | open | open |

Code Snippet

File Name kbengine/tool_operate.c
Method static CURLcode operate_do(struct GlobalConfig *global,

```
....
682.          infd = open(uploadfile, O_RDONLY | O_BINARY,
```

Potential Precision Problem

Query Path:

CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

OWASP Top 10 2017: A1-Injection

Description

Potential Precision Problem\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=545 |
| Status | New |

The size of the buffer used by flatten_match in "%s: flatten brigade", at line 94 of kbengine/testbuckets.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that flatten_match passes to "%s: flatten brigade", at line 94 of kbengine/testbuckets.c, to overwrite the target buffer.

| | Source | Destination |
|------|------------------------|------------------------|
| File | kbengine/testbuckets.c | kbengine/testbuckets.c |

| | | |
|--------|-----------------------|-----------------------|
| Line | 103 | 103 |
| Object | "%s: flatten brigade" | "%s: flatten brigade" |

Code Snippet

File Name kbengine/testbuckets.c

Method static void flatten_match(abts_case *tc, const char *ctx,

```
....  
103.      sprintf(msg, "%s: flatten brigade", ctx);
```

Potential Precision Problem\Path 2:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=546>

Status New

The size of the buffer used by flatten_match in "%s: length match (%ld not %ld)", at line 94 of kbengine/testbuckets.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that flatten_match passes to "%s: length match (%ld not %ld)", at line 94 of kbengine/testbuckets.c, to overwrite the target buffer.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | kbengine/testbuckets.c | kbengine/testbuckets.c |
| Line | 105 | 105 |
| Object | "%s: length match (%ld not %ld)" | "%s: length match (%ld not %ld)" |

Code Snippet

File Name kbengine/testbuckets.c

Method static void flatten_match(abts_case *tc, const char *ctx,

```
....  
105.      sprintf(msg, "%s: length match (%ld not %ld)", ctx,
```

Potential Precision Problem\Path 3:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=547>

Status New

The size of the buffer used by flatten_match in "%s: result match", at line 94 of kbengine/testbuckets.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that flatten_match passes to "%s: result match", at line 94 of kbengine/testbuckets.c, to overwrite the target buffer.

| | Source | Destination |
|------|------------------------|------------------------|
| File | kbengine/testbuckets.c | kbengine/testbuckets.c |

| | | |
|--------|--------------------|--------------------|
| Line | 108 | 108 |
| Object | "%s: result match" | "%s: result match" |

Code Snippet

File Name kbengine/testbuckets.c

Method static void flatten_match(abts_case *tc, const char *ctx,

```
....
108.         sprintf(msg, "%s: result match", msg);
```

Arithmenic Operation On Boolean

Query Path:

CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Arithmenic Operation On Boolean\Path 1:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=616>

Status New

| | Source | Destination |
|--------|----------------|----------------|
| File | kbengine/url.c | kbengine/url.c |
| Line | 2310 | 2310 |
| Object | BinaryExpr | BinaryExpr |

Code Snippet

File Name kbengine/url.c

Method static CURLcode parseurlandfillconn(struct Curl_easy *data,

```
....
2310.         prefixlen += 1 + (data->change.url[5] == '/');
```

Arithmenic Operation On Boolean\Path 2:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=617>

Status New

| | Source | Destination |
|------|--------------------|--------------------|
| File | kbengine/mbedtls.c | kbengine/mbedtls.c |

| | | |
|--------|------------|------------|
| Line | 655 | 655 |
| Object | BinaryExpr | BinaryExpr |

Code Snippet

File Name kbengine/mbedtls.c

Method mbedtls_connect_step2(struct connectdata *conn,

```
....
655.                                     &pubkey[PUB_DER_MAX_BYTES -
size], size);
```

Arithmetic Operation On Boolean\Path 3:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=618>

Status New

| | Source | Destination |
|--------|---------------------|---------------------|
| File | kbengine/polarssl.c | kbengine/polarssl.c |
| Line | 568 | 568 |
| Object | BinaryExpr | BinaryExpr |

Code Snippet

File Name kbengine/polarssl.c

Method polarssl_connect_step2(struct connectdata *conn,

```
....
568.                                     &pubkey[PUB_DER_MAX_BYTES -
size], size);
```

Reliance on DNS Lookups in a Decision

Query Path:

CPP\Cx\CPP Low Visibility\Reliance on DNS Lookups in a Decision Version:0

Categories

FISMA 2014: Identification And Authentication

NIST SP 800-53: SC-23 Session Authenticity (P1)

Description

Reliance on DNS Lookups in a Decision\Path 1:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2241>

Status New

The `mailer::gethostaddresses` method performs a reverse DNS lookup with `gethostbyaddr`, at line 938 of `kbengine/mailer.cpp`. The application then makes a security decision, `host`, in `kbengine/mailer.cpp` line 938, even though this hostname is not reliable and can be easily spoofed.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | <code>kbengine/mailer.cpp</code> | <code>kbengine/mailer.cpp</code> |
| Line | 945 | 949 |
| Object | <code>gethostbyaddr</code> | <code>host</code> |

Code Snippet

File Name `kbengine/mailer.cpp`

Method `bool mailer::gethostaddresses(std::vector<SOCKADDR_IN>& adds) {`

```
....
945.             host = gethostbyaddr(addr.get_sin_addr(),
sizeof(addr.ADDR.sin_addr), AF_INET);
....
949.             if(!host) { // couldn't get to dns, try to connect
directly to 'server' instead.
```

Reliance on DNS Lookups in a Decision\Path 2:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2242>

Status New

The `mailer::gethostaddresses` method performs a reverse DNS lookup with `gethostbyaddr`, at line 938 of `kbengine/mailer.cpp`. The application then makes a security decision, `host`, in `kbengine/mailer.cpp` line 938, even though this hostname is not reliable and can be easily spoofed.

| | Source | Destination |
|--------|----------------------------------|----------------------------------|
| File | <code>kbengine/mailer.cpp</code> | <code>kbengine/mailer.cpp</code> |
| Line | 957 | 962 |
| Object | <code>gethostbyaddr</code> | <code>host</code> |

Code Snippet

File Name `kbengine/mailer.cpp`

Method `bool mailer::gethostaddresses(std::vector<SOCKADDR_IN>& adds) {`

```
....
957.             host = gethostbyaddr(addr.get_sin_addr(),
sizeof(addr.ADDR.sin_addr), AF_INET);
....
962.             if(!host) {
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:

CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2145 |
| Status | New |

The system data read by krb5_auth in the file kbengine/krb5.c at line 146 is potentially exposed by krb5_auth found in kbengine/krb5.c at line 146.

| | Source | Destination |
|--------|-----------------|-----------------|
| File | kbengine/krb5.c | kbengine/krb5.c |
| Line | 171 | 171 |
| Object | perror | perror |

Code Snippet

File Name kbengine/krb5.c
Method krb5_auth(void *app_data, struct connectdata *conn)

```
....
171:      perror("getsockname()");
```

Use of Insufficiently Random Values

Query Path:

CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Insufficiently Random Values\Path 1:

| | |
|----------------|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2155 |
| Status | New |

Method Curl_ssl_random at line 736 of kbengine/vtls.c uses a weak method random to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|------|-----------------|-----------------|
| File | kbengine/vtls.c | kbengine/vtls.c |

| | | |
|--------|--------|--------|
| Line | 740 | 740 |
| Object | random | random |

Code Snippet

File Name kbengine/vtls.c

Method CURLcode Curl_ssl_random(struct Curl_easy *data,

```
....
740.     return Curl_ssl->random(data, entropy, length);
```

Privacy Violation

Query Path:

CPP\Cx\CPP Low Visibility\Privacy Violation Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure

FISMA 2014: Identification And Authentication

NIST SP 800-53: SC-4 Information in Shared Resources (P1)

OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Privacy Violation\Path 1:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1030038&projectid=30033&pathid=2156>

Status New

Method tls1_setup_key_block at line 633 of kbengine/t1_enc.c sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|--------|-------------------|-------------------|
| File | kbengine/t1_enc.c | kbengine/t1_enc.c |
| Line | 651 | 709 |
| Object | mac_secret_size | printf |

Code Snippet

File Name kbengine/t1_enc.c

Method int tls1_setup_key_block(SSL *s)

```
....
651.         (s->session, &c, &hash, &mac_type, &mac_secret_size,
&comp)) {
....
709.         printf("%02X%c", p1[z], ((z + 1) % 16) ? ' ' : '\n');
```

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 its 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 (strlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
{
    strncpy(buffer, inputString, sizeof(buffer));
}
```

Format String Attack

Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

Cause

How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

General Recommendations

How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
 - Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.
-

Source Code Examples

CPP

Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");  
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or
```

cause a crash

Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

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

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In its 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 Copy without Checking Size of Input ('Classic Buffer Overflow')

Weakness ID: 120 (*Weakness Base*)

Status: Incomplete

Description

Description Summary

The program copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow.

Extended Description

A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold, or when a program attempts to put data in a memory area outside of the boundaries of a buffer. The simplest type of error, and the most common cause of buffer overflows, is the "classic" case in which the program copies the buffer without checking its length at all. Other variants exist, but the existence of a classic overflow strongly suggests that the programmer is not considering even the most basic of security protections.

Alternate Terms

buffer overrun:

Some prominent vendors and researchers use the term "buffer overrun," but most people use "buffer overflow."

Unbounded Transfer

Terminology Notes

Many issues that are now called "buffer overflows" are substantively different than the "classic" overflow, including entirely different bug types that rely on overflow exploit techniques, such as integer signedness errors, integer overflows, and format string bugs. This imprecise terminology can make it difficult to determine which variant is being reported.

Time of Introduction

Implementation

Applicable Platforms

Languages

C

C++

Assembly

Common Consequences

| Scope | Effect |
|--------------|---|
| Integrity | <p>Technical Impact: <i>Execute unauthorized code or commands</i></p> <p>Buffer overflows often can be used to execute arbitrary code, which is usually outside the scope of a program's implicit security policy. This can often be used to subvert any other security service.</p> |
| Availability | <p>Buffer overflows generally lead to crashes. Other attacks leading to lack of availability are possible, including putting the program into an infinite loop.</p> |

Likelihood of Exploit

High to Very High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis

tool might report buffer overflows that originate from command line arguments in a program that is not expected to run with `setuid` or other special privileges.

Effectiveness: High

Detection techniques for buffer-related errors are more mature than for most other weakness types.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Manual Analysis

Manual analysis can be useful for finding this weakness, but it might not achieve desired code coverage within limited time constraints. This becomes difficult for weaknesses that must be considered for all inputs, since the attack surface can be too large.

Demonstrative Examples

Example 1

The following code asks the user to enter their last name and then attempts to store the value entered in the `last_name` array.

(Bad Code)

Example Language: C

```
char last_name[20];
printf("Enter your last name: ");
scanf("%s", last_name);
```

The problem with the code above is that it does not check the size of the name entered by the user. If the user enters "Very_very_long_last_name" which is 24 characters long, then a buffer overflow will occur since the array can only hold 20 characters total.

Example 2

The following code attempts to create a local copy of a buffer to perform some manipulations to the data.

(Bad Code)

Example Language: C

```
void manipulate_string(char* string){
char buf[24];
strcpy(buf, string);
...
}
```

However, the programmer does not ensure that the size of the data pointed to by `string` will fit in the local buffer and blindly copies the data with the potentially dangerous `strcpy()` function. This may result in a buffer overflow condition if an attacker can influence the contents of the `string` parameter.

Example 3

The excerpt below calls the `gets()` function in C, which is inherently unsafe.

(Bad Code)

Example Language: C

```
char buf[24];
printf("Please enter your name and press <Enter>\n");
gets(buf);
...
}
```

However, the programmer uses the function `gets()` which is inherently unsafe because it blindly copies all input from STDIN to the buffer without checking size. This allows the user to provide a string that is larger than the buffer size, resulting in an overflow condition.

Example 4

In the following example, a server accepts connections from a client and processes the

client request. After accepting a client connection, the program will obtain client information using the `gethostbyaddr` method, copy the hostname of the client that connected to a local variable and output the hostname of the client to a log file.

(Bad Code)

Example Languages: C and C++

```
...
struct hostent *clienthp;
char hostname[MAX_LEN];

// create server socket, bind to server address and listen on socket
...

// accept client connections and process requests
int count = 0;
for (count = 0; count < MAX_CONNECTIONS; count++) {

int clientlen = sizeof(struct sockaddr_in);
int clientsocket = accept(serversocket, (struct sockaddr *)&clientaddr, &clientlen);

if (clientsocket >= 0) {
clienthp = gethostbyaddr((char *)&clientaddr.sin_addr.s_addr,
sizeof(clientaddr.sin_addr.s_addr), AF_INET);
strcpy(hostname, clienthp->h_name);
logOutput("Accepted client connection from host ", hostname);

// process client request
...
close(clientsocket);
}
}
close(serversocket);
...
```

However, the hostname of the client that connected may be longer than the allocated size for the local hostname variable. This will result in a buffer overflow when copying the client hostname to the local variable using the `strcpy` method.

Observed Examples

| Reference | Description |
|-------------------------------|--|
| CVE-2000-1094 | buffer overflow using command with long argument |
| CVE-1999-0046 | buffer overflow in local program using long environment variable |
| CVE-2002-1337 | buffer overflow in comment characters, when product increments a counter for a ">" but does not decrement for "<" |
| CVE-2003-0595 | By replacing a valid cookie value with an extremely long string of characters, an attacker may overflow the application's buffers. |
| CVE-2001-0191 | By replacing a valid cookie value with an extremely long string of characters, an attacker may overflow the application's buffers. |

Potential Mitigations

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate buffer overflows.

For example, many languages that perform their own memory management, such as Java and Perl, are not subject to buffer overflows. Other languages, such as Ada and C#, typically provide overflow protection, but the protection can be disabled by the programmer.

Be wary that a language's interface to native code may still be subject to overflows, even if the language itself is theoretically safe.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Examples include the Safe C String Library (SafeStr) by Messier and Viega, and the Strsafe.h library from Microsoft. These libraries provide safer versions of overflow-prone string-handling functions. This is not a complete solution, since many buffer overflows are not related to strings.

Phase: Build and Compilation

Run or compile your software using features or extensions that automatically provide a protection mechanism that mitigates or eliminates buffer overflows.

For example, certain compilers and extensions provide automatic buffer overflow detection mechanisms that are built into the compiled code. Examples include the Microsoft Visual Studio /GS flag, Fedora/Red Hat FORTIFY_SOURCE GCC flag, StackGuard, and ProPolice.

This is not necessarily a complete solution, since these mechanisms can only detect certain types of overflows. In addition, a buffer overflow attack can still cause a denial of service, since the typical response is to exit the application.

Phase: Implementation

Programmers should adhere to the following rules when allocating and managing their applications memory:

- Double check that your buffer is as large as you specify.
- When using functions that accept a number of bytes to copy, such as strncpy(), be aware that if the destination buffer size is equal to the source buffer size, it may not NULL-terminate the string.
- Check buffer boundaries if calling this function in a loop and make sure you are not in danger of writing past the allocated space.
- If necessary, truncate all input strings to a reasonable length before passing them to the copy and concatenation functions.

Phase: Operation

Use a feature like Address Space Layout Randomization (ASLR). This is not a complete solution. However, it forces the attacker to guess an unknown value that changes every program execution.

Phase: Operation

Use a CPU and operating system that offers Data Execution Protection (NX) or its equivalent. This is not a complete solution, since buffer overflows could be used to overwrite nearby variables to modify the software's state in dangerous ways. In addition, it cannot be used in cases in which self-modifying code is required.

Phases: Build and Compilation; Operation

Most mitigating technologies at the compiler or OS level to date address only a subset of buffer overflow problems and rarely provide complete protection against even that subset. It is good practice to implement strategies to increase the workload of an attacker, such as leaving the attacker to guess an unknown value that changes every program execution.

Phase: Implementation

Replace unbounded copy functions with analogous functions that support length arguments, such as strcpy with strncpy. Create these if they are not available.

Effectiveness: Moderate

This approach is still susceptible to calculation errors, including issues such as off-by-one errors (CWE-193) and incorrectly calculating buffer lengths (CWE-131).

Weakness Ordinalities

| Ordinality | Description |
|------------|---|
| Resultant | <i>(where the weakness is typically related to the presence of some other weaknesses)</i> |
| Primary | <i>(where the weakness exists independent of other weaknesses)</i> |

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---------|----------------|-----|--|--|
| ChildOf | Weakness Class | 20 | Improper Input Validation | Seven Pernicious Kingdoms (primary)700 |
| ChildOf | Weakness Class | 119 | Failure to Constrain Operations within the Bounds of a Memory Buffer | Development Concepts (primary)699 Research Concepts (primary)1000 |

| | | | | |
|------------|------------------|-----|--|--|
| ChildOf | Category | 633 | Weaknesses that Affect Memory | Resource-specific Weaknesses (primary)631 |
| ChildOf | Category | 722 | OWASP Top Ten 2004 Category A1 - Unvalidated Input | Weaknesses in OWASP Top Ten (2004)711 |
| ChildOf | Category | 726 | OWASP Top Ten 2004 Category A5 - Buffer Overflows | Weaknesses in OWASP Top Ten (2004) (primary)711 |
| ChildOf | Category | 741 | CERT C Secure Coding Section 07 - Characters and Strings (STR) | Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734 |
| ChildOf | Category | 802 | 2010 Top 25 - Risky Resource Management | Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800 |
| CanPrecede | Weakness Base | 123 | Write-what-where Condition | Research Concepts1000 |
| ParentOf | Weakness Variant | 785 | Use of Path Manipulation Function without Maximum-sized Buffer | Development Concepts (primary)699 |
| CanFollow | Weakness Base | 170 | Improper Null Termination | Research Concepts1000 |
| CanFollow | Weakness Base | 231 | Improper Handling of Extra Values | Research Concepts1000 |
| CanFollow | Weakness Base | 242 | Use of Inherently Dangerous Function | Research Concepts1000 |
| CanFollow | Weakness Base | 416 | Use After Free | Research Concepts1000 |
| CanFollow | Weakness Base | 456 | Missing Initialization | Research Concepts1000 |
| PeerOf | Weakness Base | 124 | Buffer Underwrite ('Buffer Underflow') | Research Concepts1000 |
| CanAlsoBe | Weakness Variant | 196 | Unsigned to Signed Conversion Error | Research Concepts1000 |

Relationship Notes

At the code level, stack-based and heap-based overflows do not differ significantly, so there usually is not a need to distinguish them. From the attacker perspective, they can be quite different, since different techniques are required to exploit them.

Affected Resources

- Memory

Functional Areas

- Memory Management

f Causal Nature

Explicit

Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|-----------------------|---------|-------------------|---|
| PLOVER | | | Unbounded Transfer ('classic overflow') |
| 7 Pernicious Kingdoms | | | Buffer Overflow |
| CLASP | | | Buffer overflow |
| OWASP Top Ten 2004 | A1 | CWE More Specific | Unvalidated Input |
| OWASP Top Ten 2004 | A5 | CWE More Specific | Buffer Overflows |
| CERT C Secure Coding | STR35-C | | Do not copy data from an unbounded source to a fixed-length array |
| WASC | 7 | | Buffer Overflow |

Related Attack Patterns

| CAPEC-ID | Attack Pattern Name | (CAPEC Version: 1.5) |
|---------------------|---|----------------------|
| 8 | Buffer Overflow in an API Call | |
| 9 | Buffer Overflow in Local Command-Line Utilities | |
| 10 | Buffer Overflow via Environment Variables | |
| 14 | Client-side Injection-induced Buffer Overflow | |
| 24 | Filter Failure through Buffer Overflow | |
| 92 | Forced Integer Overflow | |
| 42 | MIME Conversion | |
| 44 | Overflow Binary Resource File | |
| 45 | Buffer Overflow via Symbolic Links | |
| 100 | Overflow Buffers | |
| 46 | Overflow Variables and Tags | |
| 47 | Buffer Overflow via Parameter Expansion | |
| 67 | String Format Overflow in syslog() | |

White Box Definitions

A weakness where the code path includes a Buffer Write Operation such that:

1. the expected size of the buffer is greater than the actual size of the buffer where expected size is equal to the sum of the size of the data item and the position in the buffer

Where Buffer Write Operation is a statement that writes a data item of a certain size into a buffer at a certain position and at a certain index

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Public Enemy #1: The Buffer Overrun" Page 127. 2nd Edition. Microsoft. 2002.

[REF-17] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 5: Buffer Overruns." Page 89. McGraw-Hill. 2010.

Microsoft. "Using the Strsafe.h Functions". <<http://msdn.microsoft.com/en-us/library/ms647466.aspx>>.

Matt Messier and John Viega. "Safe C String Library v1.0.3". <<http://www.zork.org/safestr/>>.

Michael Howard. "Address Space Layout Randomization in Windows Vista". <http://blogs.msdn.com/michael_howard/archive/2006/05/26/address-space-layout-randomization-in-windows-vista.aspx>.

Arjan van de Ven. "Limiting buffer overflows with ExecShield". <<http://www.redhat.com/magazine/009jul05/features/execshield/>>.

"PaX". <<http://en.wikipedia.org/wiki/PaX>>.

Content History

| Submissions | | | |
|-------------------|--|---------------|------------------|
| Submission Date | Submitter | Organization | Source |
| | PLOVER | | Externally Mined |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Time of Introduction | | |
| 2008-08-01 | | KDM Analytics | External |
| | added/updated white box definitions | | |
| 2008-08-15 | | Veracode | External |
| | Suggested OWASP Top Ten 2004 mapping | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Observed Example, Other Notes, Taxonomy Mappings, Weakness Ordinalities | | |
| 2008-10-10 | CWE Content Team | MITRE | Internal |

| | | | |
|------------|--|-------|----------|
| | Changed name and description to more clearly emphasize the "classic" nature of the overflow. | | |
| 2008-10-14 | CWE Content Team | MITRE | Internal |
| | updated Alternate Terms, Description, Name, Other Notes, Terminology Notes | | |
| 2008-11-24 | CWE Content Team | MITRE | Internal |
| | updated Other Notes, Relationships, Taxonomy Mappings | | |
| 2009-01-12 | CWE Content Team | MITRE | Internal |
| | updated Common Consequences, Other Notes, Potential Mitigations, References, Relationship Notes, Relationships | | |
| 2009-07-27 | CWE Content Team | MITRE | Internal |
| | updated Other Notes, Potential Mitigations, Relationships | | |
| 2009-10-29 | CWE Content Team | MITRE | Internal |
| | updated Common Consequences, Relationships | | |
| 2010-02-16 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Potential Mitigations, References, Related Attack Patterns, Relationships, Taxonomy Mappings, Time of Introduction, Type | | |
| 2010-04-05 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples, Related Attack Patterns | | |

Previous Entry Names

| Change Date | Previous Entry Name |
|-------------|--|
| 2008-10-14 | Unbounded Transfer ('Classic Buffer Overflow') |

[BACK TO TOP](#)

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 its 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 OutOfBound

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 its most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

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

General Recommendations

How to avoid it

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

Source Code Examples

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
 - Review code to ensure no flow allows use of a pointer after it has been explicitly freed
-

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);  
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()  
{  
    int i;  
    i = 1;  
    return &i;  
}  
  
void func2()  
{  
    int j;  
    j = 5;
```

```
}

//..
    int * i = func1();
    printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
    func2();
    printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

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

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In its 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

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occurring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
 - Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
 - Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
 - Ensure divide-by-zero errors are caught and handled appropriately.
-

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {  
    int total = Integer.parseInt(req.getParameter("total"));  
    int count = Integer.parseInt(req.getParameter("count"));  
  
    return total / count;  
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {  
    int total = Integer.parseInt(req.getParameter("total"));  
    int count = Integer.parseInt(req.getParameter("count"));  
  
    if (count > 0)  
        return total / count;  
    else
```

```
}      return 0;
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g. memory) that may be exploited.

Cause

How does it happen

Calling `free()` on a variable that was not dynamically allocated (e.g. `malloc`) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use `free()` only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling `free()` on a static variable

```
void clean_up() {  
    char temp[256];  
    do_something();  
    free(tmp);  
    return;  
}
```

Good - Calling `free()` only on variables that were dynamically allocated

```
void clean_up() {  
    char *buff;  
    buff = (char*) malloc(1024);  
    free(buff);  
    return;  
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
 - Specifically for memory allocation, calculate the allocation size from the allocation source:
 - Derive the size value from the length of intended source to determine the amount of units to be processed.
 - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using `sizeof()` on the unit's type.
 - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.
-

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
    ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
    ptr[i] = i * 2 + 1;
}
```



```
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;  
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"  
wcscpy((wchar_t *)dest, source);  
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;  
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));  
wcscpy((wchar_t *)dest, source);  
wprintf(L"Dest: %s\r\n", dest);
```

Boolean Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
 - Prefer promoting the target variable to a large enough data type.
 - If downcasting is necessary, always check that values are valid and in range of the target type, before casting
-

Source Code Examples

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
 - Prefer promoting the target variable to a large enough data type.
 - If downcasting is necessary, always check that values are valid and in range of the target type, before casting
-

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {  
  
    // op2 gets forced from int into a short  
    short total = op1 + op2;  
  
    return total;  
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {  
  
    // total variable is of type int, the largest type that is needed  
    int total = 0;  
  
    // check if total will overflow available integer size  
    if (INT_MAX - abs(op2) > op1)  
    {  
        total = op1 + op2;  
    }  
    else
```

```
{  
    // instead of overflow, saturate (but this is not always a good thing)  
    total = INT_MAX  
}  
  
return total;  
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
 - Prefer promoting the target variable to a large enough data type.
 - If downcasting is necessary, always check that values are valid and in range of the target type, before casting
-

Source Code Examples

Long Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
 - Prefer promoting the target variable to a large enough data type.
 - If downcasting is necessary, always check that values are valid and in range of the target type, before casting
-

Source Code Examples

Short Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
 - Prefer promoting the target variable to a large enough data type.
 - If downcasting is necessary, always check that values are valid and in range of the target type, before casting
-

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
 - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
 - Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.
-

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
    char buf[10];

    printf("Please enter your name: ");
    gets(buf); // veryveryverylongname
    if (buf == ACCEPTED_NAME)
    {
        // Do something
    }
    return 0;
}
```

Safe reading from user


```
int main()
{
    char buf[10];

    printf("Please enter your name: ");
    fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
    if (buf == ACCEPTED_NAME)
    {
        //Do something
    }
    return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
    char buf[10];
    strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

    return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
    char buf[10];
    strncpy(buf, argv[1], sizeof(buf));
    buf[9]= '\0'; //strncpy doesn't NULL terminates

    return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
    printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause an access violation
    return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
    printf("%s", argv[1]); // Second parameter is not a formattable string

    return 0;
}
```

Double Free

Weakness ID: 415 (*Weakness Variant*)

Status: Draft

Description

Description Summary

The product calls `free()` twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls `free()` twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to `malloc()` to return the same pointer. If `malloc()` returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

| Scope | Effect |
|----------------|---|
| Access Control | Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code. |

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: C

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
    free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: C

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
    char *buf1R1;
    char *buf2R1;
    char *buf1R2;
    buf1R1 = (char *) malloc(BUFSIZE2);
    buf2R1 = (char *) malloc(BUFSIZE2);
    free(buf1R1);
    free(buf2R1);
    buf1R2 = (char *) malloc(BUFSIZE1);
    strncpy(buf1R2, argv[1], BUFSIZE1-1);
    free(buf2R1);
    free(buf1R2);
}
```

Observed Examples

| Reference | Description |
|-------------------------------|--|
| CVE-2004-0642 | Double free resultant from certain error conditions. |
| CVE-2004-0772 | Double free resultant from certain error conditions. |
| CVE-2005-1689 | Double free resultant from certain error conditions. |
| CVE-2003-0545 | Double free from invalid ASN.1 encoding. |
| CVE-2003-1048 | Double free from malformed GIF. |
| CVE-2005-0891 | Double free from malformed GIF. |
| CVE-2002-0059 | Double free from malformed compressed data. |

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---------|----------------|-----|---|--|
| ChildOf | Weakness Class | 398 | Indicator of Poor Code Quality | Seven Pernicious Kingdoms (primary)700 |
| ChildOf | Category | 399 | Resource Management Errors | Development Concepts (primary)699 |
| ChildOf | Category | 633 | Weaknesses that Affect Memory | Resource-specific Weaknesses (primary)631 |
| ChildOf | Weakness Base | 666 | Operation on Resource in Wrong Phase of | Research Concepts (primary)1000 |

| | | | | |
|----------|----------------|-----|---|---|
| ChildOf | Weakness Class | 675 | Lifetime Duplicate Operations on Resource | Research Concepts1000 |
| ChildOf | Category | 742 | CERT C Secure Coding Section 08 - Memory Management (MEM) | Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734 |
| PeerOf | Weakness Base | 123 | Write-what-where Condition | Research Concepts1000 |
| PeerOf | Weakness Base | 416 | Use After Free | Development Concepts699 Research Concepts1000 |
| MemberOf | View | 630 | Weaknesses Examined by SAMATE | Weaknesses Examined by SAMATE (primary)630 |
| PeerOf | Weakness Base | 364 | Signal Handler Race Condition | Research Concepts1000 |

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

Memory

Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|-----------------------|---------|-----|---|
| PLOVER | | | DFREE - Double-Free Vulnerability |
| 7 Pernicious Kingdoms | | | Double Free |
| CLASP | | | Doubly freeing memory |
| CERT C Secure Coding | MEM00-C | | Allocate and free memory in the same module, at the same level of abstraction |
| CERT C Secure Coding | MEM01-C | | Store a new value in pointers immediately after free() |
| CERT C Secure Coding | MEM31-C | | Free dynamically allocated memory exactly once |

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

| Submissions | | | |
|-------------------|--|---------------|------------------|
| Submission Date | Submitter | Organization | Source |
| | PLOVER | | Externally Mined |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Potential Mitigations, Time of Introduction | | |
| 2008-08-01 | | KDM Analytics | External |
| | added/updated white box definitions | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings | | |
| 2008-11-24 | CWE Content Team | MITRE | Internal |

| | | | |
|------------|--|-------|----------|
| | updated Relationships, Taxonomy Mappings | | |
| 2009-05-27 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |
| 2009-10-29 | CWE Content Team | MITRE | Internal |
| | updated Other Notes | | |

[BACK TO TOP](#)

Improper Sanitization of Special Elements used in a Command ('Command Injection')

Weakness ID: 77 (*Weakness Class*)

Status: Draft

Description

Description Summary

The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not sanitize or incorrectly sanitizes special elements that could modify the intended command when it is sent to a downstream component.

Extended Description

Command injection vulnerabilities typically occur when:

1. Data enters the application from an untrusted source.
2. The data is part of a string that is executed as a command by the application.
3. By executing the command, the application gives an attacker a privilege or capability that the attacker would not otherwise have.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Common Consequences

| Scope | Effect |
|----------------|---|
| Access Control | Command injection allows for the execution of arbitrary commands and code by the attacker. |
| Integrity | If a malicious user injects a character (such as a semi-colon) that delimits the end of one command and the beginning of another, it may be possible to then insert an entirely new and unrelated command that was not intended to be executed. |

Likelihood of Exploit

Very High

Demonstrative Examples

Example 1

The following simple program accepts a filename as a command line argument and displays the contents of the file back to the user. The program is installed setuid root because it is intended for use as a learning tool to allow system administrators in-training to inspect privileged system files without giving them the ability to modify them or damage the system.

Example Language: C

```
int main(char* argc, char** argv) {
    char cmd[CMD_MAX] = "/usr/bin/cat ";
    strcat(cmd, argv[1]);
    system(cmd);
}
```

Because the program runs with root privileges, the call to `system()` also executes with root privileges. If a user specifies a standard filename, the call works as expected. However, if an attacker passes a string of the form `";rm -rf /"`, then the call to `system()` fails to execute `cat` due to a lack of arguments and then plows on to recursively delete

the contents of the root partition.

Example 2

The following code is from an administrative web application designed to allow users to kick off a backup of an Oracle database using a batch-file wrapper around the rman utility and then run a cleanup.bat script to delete some temporary files. The script rmanDB.bat accepts a single command line parameter, which specifies what type of backup to perform. Because access to the database is restricted, the application runs the backup as a privileged user.

(Bad Code)

Example Language: Java

```
...
String btype = request.getParameter("backuptype");
String cmd = new String("cmd.exe /K \"
c:\\util\\rmanDB.bat \"
+btype+
"&&c:\\util\\cleanup.bat\"")
System.Runtime.getRuntime().exec(cmd);
...
```

The problem here is that the program does not do any validation on the backuptype parameter read from the user. Typically the Runtime.exec() function will not execute multiple commands, but in this case the program first runs the cmd.exe shell in order to run multiple commands with a single call to Runtime.exec(). Once the shell is invoked, it will happily execute multiple commands separated by two ampersands. If an attacker passes a string of the form "& del c:\\dbms*.\"", then the application will execute this command along with the others specified by the program. Because of the nature of the application, it runs with the privileges necessary to interact with the database, which means whatever command the attacker injects will run with those privileges as well.

Example 3

The following code from a system utility uses the system property APPHOME to determine the directory in which it is installed and then executes an initialization script based on a relative path from the specified directory.

(Bad Code)

Example Language: Java

```
...
String home = System.getProperty("APPHOME");
String cmd = home + INITCMD;
java.lang.Runtime.getRuntime().exec(cmd);
...
```

The code above allows an attacker to execute arbitrary commands with the elevated privilege of the application by modifying the system property APPHOME to point to a different path containing a malicious version of INITCMD. Because the program does not validate the value read from the environment, if an attacker can control the value of the system property APPHOME, then they can fool the application into running malicious code and take control of the system.

Example 4

The following code is from a web application that allows users access to an interface through which they can update their password on the system. Part of the process for updating passwords in certain network environments is to run a make command in the /var/yp directory, the code for which is shown below.

(Bad Code)

Example Language: Java

```
...
System.Runtime.getRuntime().exec("make");
...
```

The problem here is that the program does not specify an absolute path for make and fails to clean its environment prior to executing the call to Runtime.exec(). If an attacker can modify the \$PATH variable to point to a malicious binary called make and cause the program to be executed in their environment, then the malicious binary will be loaded instead of the one intended. Because of the nature of the application, it runs with the privileges necessary to perform system operations, which means the attacker's make will now be run with these privileges, possibly giving the attacker complete control of the system.

Example 5

The following code is a wrapper around the UNIX command cat which prints the contents of a file to standard out. It is also injectable:

(Bad Code)

Example Language: C

```
#include <stdio.h>
#include <unistd.h>

int main(int argc, char **argv) {

char cat[] = "cat ";
char *command;
size_t commandLength;

commandLength = strlen(cat) + strlen(argv[1]) + 1;
command = (char *) malloc(commandLength);
strncpy(command, cat, commandLength);
strncat(command, argv[1], (commandLength - strlen(cat)) );

system(command);
return (0);
}
```

Used normally, the output is simply the contents of the file requested:

```
$ ./catWrapper Story.txt
When last we left our heroes...
```

However, if we add a semicolon and another command to the end of this line, the command is executed by catWrapper with no complaint:

(Attack)

```
$ ./catWrapper Story.txt; ls
When last we left our heroes...
Story.txt
SensitiveFile.txt
PrivateData.db
a.out*
```

If catWrapper had been set to have a higher privilege level than the standard user, arbitrary commands could be executed with that higher privilege.

Potential Mitigations

Phase: Architecture and Design

If at all possible, use library calls rather than external processes to recreate the desired functionality

Phase: Implementation

If possible, ensure that all external commands called from the program are statically created.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists

can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."

Run time: Run time policy enforcement may be used in a white-list fashion to prevent use of any non-sanctioned commands.

Assign permissions to the software system that prevents the user from accessing/opening privileged files.

Other Notes

Command injection is a common problem with wrapper programs.

Weakness Ordinalities

| Ordinality | Description |
|------------|---|
| Primary | (where the weakness exists independent of other weaknesses) |

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|----------|----------------|-----|--|--|
| ChildOf | Weakness Class | 20 | Improper Input Validation | Seven Pernicious Kingdoms (primary)700 |
| ChildOf | Weakness Class | 74 | Failure to Sanitize Data into a Different Plane ('Injection') | Development Concepts (primary)699 |
| ChildOf | Category | 713 | OWASP Top Ten 2007 Category A2 - Injection Flaws | Research Concepts (primary)1000 |
| ChildOf | Category | 722 | OWASP Top Ten 2004 Category A1 - Unvalidated Input | Weaknesses in OWASP Top Ten (2007) (primary)629 |
| ChildOf | Category | 727 | OWASP Top Ten 2004 Category A6 - Injection Flaws | Weaknesses in OWASP Top Ten (2004) (primary)711 |
| ParentOf | Weakness Base | 78 | Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection') | Development Concepts (primary)699 |
| ParentOf | Weakness Base | 88 | Argument Injection or Modification | Research Concepts (primary)1000 |
| ParentOf | Weakness Base | 89 | Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection') | Development Concepts (primary)699 |
| ParentOf | Weakness Base | 90 | Failure to Sanitize Data into LDAP Queries ('LDAP Injection') | Research Concepts (primary)1000 |
| ParentOf | Weakness Base | 624 | Executable Regular Expression Error | Development Concepts (primary)699 |
| | | | | Research Concepts (primary)1000 |

f Causal Nature

Explicit

Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|-----------------------|---------|-----|-------------------|
| 7 Pernicious Kingdoms | | | Command Injection |
| CLASP | | | Command injection |

| | | | |
|--------------------|----|-------------------|-------------------|
| OWASP Top Ten 2007 | A2 | CWE More Specific | Injection Flaws |
| OWASP Top Ten 2004 | A1 | CWE More Specific | Unvalidated Input |
| OWASP Top Ten 2004 | A6 | CWE More Specific | Injection Flaws |

Related Attack Patterns

| CAPEC-ID | Attack Pattern Name | (CAPEC Version: 1.5) |
|--------------------|---|----------------------|
| 15 | Command Delimiters | |
| 23 | File System Function Injection, Content Based | |
| 43 | Exploiting Multiple Input Interpretation Layers | |
| 75 | Manipulating Writeable Configuration Files | |
| 6 | Argument Injection | |
| 11 | Cause Web Server Misclassification | |
| 76 | Manipulating Input to File System Calls | |

References

G. Hoglund and G. McGraw. "Exploiting Software: How to Break Code". Addison-Wesley. February 2004.

Content History

| Submissions | | | |
|----------------------|---|--------------|------------------|
| Submission Date | Submitter | Organization | Source |
| | 7 Pernicious Kingdoms | | Externally Mined |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2008-07-01 | Eric Dalci updated Time of Introduction | Cigital | External |
| 2008-08-15 | | Veracode | External |
| 2008-09-08 | Suggested OWASP Top Ten 2004 mapping CWE Content Team updated Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities | MITRE | Internal |
| 2009-05-27 | CWE Content Team updated Demonstrative Examples, Name | MITRE | Internal |
| 2009-07-27 | CWE Content Team updated Demonstrative Examples, Description, Name | MITRE | Internal |
| 2009-10-29 | CWE Content Team updated Common Consequences, Description, Other Notes, Potential Mitigations | MITRE | Internal |
| 2010-02-16 | CWE Content Team updated Potential Mitigations, Relationships | MITRE | Internal |
| Previous Entry Names | | | |
| Change Date | Previous Entry Name | | |
| 2008-04-11 | Command Injection | | |
| 2009-05-27 | Failure to Sanitize Data into a Control Plane (aka 'Command Injection') | | |
| 2009-07-27 | Failure to Sanitize Data into a Control Plane ('Command Injection') | | |

[BACK TO TOP](#)

Use of Hard coded Cryptographic Key

Risk

What might happen

Static, unchangeable encryption keys in the source code can be stolen by an attacker with access to the source code or the application binaries. Once the attacker has the encryption key, this can be used to gain access to any encrypted secret data, thus violating the confidentiality of the data. Furthermore, it would be impossible to replace the encryption key once stolen. Note that if this is a product that can be installed numerous times, the encryption key will always be the same, allowing an attacker to break all instances at the same cost.

Cause

How does it happen

The application code uses an encryption key to encrypt and decrypt sensitive data. While it is important to create this encryption key randomly and keep it secret, the application has a single, static key embedded in plain text in the source code.

An attacker could gain access to the source code - whether in the source control system, developer workstations, or the server filesystem or product binaries themselves. Once the attacker has gained access to the source code, it is trivial to retrieve the plain text encryption key and use it to decrypt the sensitive data that the application was protecting.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store any sensitive information, such as encryption keys, in plain text.
- Never hardcode encryption keys in the application source code.
- Implement proper key management, including dynamically generating random keys, protecting keys, and replacing keys as necessary.

Specific Recommendations:

- Remove the hardcoded encryption key from the application source code. Instead, retrieve the key from an external, protected store.
-

Source Code Examples

Java

Common example of hardcoded encryption key

```
//Generate a key
string encryptionKey = "EncryptionKey123"

//Encrypt the data
SecretKeySpec keySpec = new SecretKeySpec(encryptionKey.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
cipher.init(Cipher.ENCRYPT_MODE, keySpec);
output = cipher.doFinal(input)
```


Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privileged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.

Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store sensitive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as `SealedObject`.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as `SecureString` or `ProtectedData`.
-

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
    private string password;

    void setPassword()
```

```
{  
    password = System.console().readLine("Enter your password: ");  
}  
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed  
{  
    private SealedObject password;  
  
    void setPassword()  
    {  
        byte[] sKey = getKeyFromConfig();  
        Cipher c = Cipher.getInstance("AES");  
        c.init(Cipher.ENCRYPT_MODE, sKey);  
  
        char[] input = System.console().readPassword("Enter your password: ");  
        password = new SealedObject(Arrays.asList(input), c);  
  
        //Zero out the possible password, for security.  
        Arrays.fill(password, '0');  
    }  
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */  
  
#include <stdio.h>  
  
void somefunc() {  
    printf("Yea, I'm just being called for the heap of it..\n");  
}  
  
void authfunc() {  
    char* password = (char *) malloc(256);  
    char ch;  
    ssize_t k;  
    int i=0;  
    while(k = read(0, &ch, 1) > 0)  
    {  
        if (ch == '\n') {  
            password[i]='\0';  
            break;  
        } else {  
            password[i++]=ch;  
            fflush(0);  
        }  
    }  
    printf("Password: %s\n", &password[0]);  
}  
  
int main()  
{  
    printf("Please enter a password:\n");  
  
    authfunc();  
    printf("You can now dump memory to find this password!");  
    somefunc();  
}
```

```
    gets();  
  
}
```

Safe C code

```
/* Presumably safe heap */  
  
#include <stdio.h>  
#include <string.h>  
  
#define STDIN_FILENO 0  
  
void somefunc() {  
    printf("Yea, I'm just being called for the heap of it..\n");  
}  
  
void authfunc() {  
    char* password = (char*) malloc(256);  
    int i=0;  
    char ch;  
    ssize_t k;  
    while(k = read(STDIN_FILENO, &ch, 1) > 0)  
    {  
        if (ch == '\n') {  
            password[i]='\0';  
            break;  
        } else {  
            password[i++]=ch;  
            fflush(0);  
        }  
    }  
    i=0;  
    memset(password, '\0', 256);  
}  
  
int main()  
{  
  
    printf("Please enter a password:\n");  
    authfunc();  
    somefunc();  
    char ch;  
    while(read(STDIN_FILENO, &ch, 1) > 0)  
    {  
        if (ch == '\n')  
            break;  
    }  
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')**Weakness ID:** 401 (*Weakness Base*)**Status:** Draft**Description****Description Summary**

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms**Languages**

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

| Scope | Effect |
|--------------|---|
| Availability | Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition. |

Likelihood of Exploit

Medium

Demonstrative Examples**Example 1**

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

*(Bad Code)**Example Language: C*

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```



```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: C

```
bar connection(){
foo = malloc(1024);
return foo;
}

endConnection(bar foo) {

free(foo);
}

int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

| Reference | Description |
|-------------------------------|--|
| CVE-2005-3119 | Memory leak because function does not free() an element of a data structure. |
| CVE-2004-0427 | Memory leak when counter variable is not decremented. |
| CVE-2002-0574 | Memory leak when counter variable is not decremented. |
| CVE-2005-3181 | Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code. |
| CVE-2004-0222 | Memory leak via unknown manipulations as part of protocol test suite. |
| CVE-2001-0136 | Memory leak via a series of the same command. |

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---------|----------------|-----|--|--|
| ChildOf | Weakness Class | 398 | Indicator of Poor Code Quality | Seven Pernicious Kingdoms (primary)700 |
| ChildOf | Category | 399 | Resource Management Errors | Development Concepts (primary)699 |
| ChildOf | Category | 633 | Weaknesses that Affect Memory | Resource-specific Weaknesses (primary)631 |
| ChildOf | Category | 730 | OWASP Top Ten 2004 Category A9 - Denial of Service | Weaknesses in OWASP Top Ten (2004) (primary)711 |
| ChildOf | Weakness Base | 772 | Missing Release of Resource after Effective | Research Concepts (primary)1000 |

| | | | | |
|-----------|----------------|-----|---|---|
| MemberOf | View | 630 | Lifetime Weaknesses Examined by SAMATE | Weaknesses Examined by SAMATE (primary) 630 Research Concepts1000 |
| CanFollow | Weakness Class | 390 | Detection of Error Condition Without Action | |

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|-----------------------|---------|-------------------|----------------------------|
| PLOVER | | | Memory leak |
| 7 Pernicious Kingdoms | | | Memory Leak |
| CLASP | | | Failure to deallocate data |
| OWASP Top Ten 2004 | A9 | CWE More Specific | Denial of Service |

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource
2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained
2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element
3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release
4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

| Submissions | | | |
|-------------------|---|---------------|------------------|
| Submission Date | Submitter | Organization | Source |
| | PLOVER | | Externally Mined |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Time of Introduction | | |
| 2008-08-01 | | KDM Analytics | External |
| | added/updated white box definitions | | |
| 2008-08-15 | | Veracode | External |
| | Suggested OWASP Top Ten 2004 mapping | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes | | |
| 2008-10-14 | CWE Content Team | MITRE | Internal |
| | updated Description | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |
| | updated Other Notes | | |
| 2009-05-27 | CWE Content Team | MITRE | Internal |
| | updated Name | | |
| 2009-07-17 | KDM Analytics | | External |
| | Improved the White Box Definition | | |

| | | | | |
|----------------------|--|-------|----------|--|
| 2009-07-27 | CWE Content Team | MITRE | Internal | |
| | updated White Box Definitions | | | |
| 2009-10-29 | CWE Content Team | MITRE | Internal | |
| | updated Modes of Introduction, Other Notes | | | |
| 2010-02-16 | CWE Content Team | MITRE | Internal | |
| | updated Relationships | | | |
| Previous Entry Names | | | | |
| Change Date | Previous Entry Name | | | |
| 2008-04-11 | Memory Leak | | | |
| 2009-05-27 | Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak') | | | |

[BACK TO TOP](#)

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
 - Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
 - Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.
-

Source Code Examples

Use of Uninitialized Variable

Weakness ID: 457 (Weakness Variant)

Status: Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

Implementation

Applicable Platforms

Languages

C: (Sometimes)

C++: (Sometimes)

Perl: (Often)

All

Common Consequences

| Scope | Effect |
|---------------------------|---|
| Availability Integrity | Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not. |
| Authorization | Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end - of a string. |

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: C

```
switch (ctl) {  
case -1:  
aN = 0;  
bN = 0;  
break;  
case 0:  
aN = i;  
bN = -i;  
break;  
case 1:  
aN = i + NEXT_SZ;  
bN = i - NEXT_SZ;  
break;  
default:  
aN = 0;  
bN = 0;  
break;  
}
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: C++ and Java

```
int foo;
void bar() {
if (foo==0)
/.../
/..//
}
```

Observed Examples

| Reference | Description |
|-------------------------------|--|
| CVE-2008-0081 | Uninitialized variable leads to code execution in popular desktop application. |
| CVE-2007-4682 | Crafted input triggers dereference of an uninitialized object pointer. |
| CVE-2007-3468 | Crafted audio file triggers crash when an uninitialized variable is used. |
| CVE-2007-2728 | Uninitialized random seed variable used. |

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---------|----------------|-----|--|--|
| ChildOf | Weakness Class | 398 | Indicator of Poor Code Quality | Seven Pernicious Kingdoms (primary)700 |
| ChildOf | Weakness Base | 456 | Missing Initialization | Development Concepts (primary)699 Research Concepts |

| | | | | |
|----------|------|-----|---|---|
| MemberOf | View | 630 | Weaknesses Examined by SAMATE | (primary)1000 Weaknesses Examined by SAMATE (primary)630 |
|----------|------|-----|---|---|

Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|-----------------------|---------|-----|------------------------|
| CLASP | | | Uninitialized variable |
| 7 Pernicious Kingdoms | | | Uninitialized Variable |

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. <<http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <<http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>>.

Content History

| Submissions | | | |
|----------------------|---|---------------|------------------|
| Submission Date | Submitter | Organization | Source |
| | CLASP | | Externally Mined |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Time of Introduction | | |
| 2008-08-01 | | KDM Analytics | External |
| | added/updated white box definitions | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings | | |
| 2009-01-12 | CWE Content Team | MITRE | Internal |
| | updated Common Consequences, Demonstrative Examples, Potential Mitigations | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |
| 2009-05-27 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |
| Previous Entry Names | | | |
| Change Date | Previous Entry Name | | |
| 2008-04-11 | Uninitialized Variable | | |

[BACK TO TOP](#)

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
 - Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
 - Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.
-

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```




Inadequate Encryption Strength

Risk

What might happen

Using weak or outdated cryptography does not provide sufficient protection for sensitive data. An attacker that gains access to the encrypted data would likely be able to break the encryption, using either cryptanalysis or brute force attacks. Thus, the attacker would be able to steal user passwords and other personal data. This could lead to user impersonation or identity theft.

Cause

How does it happen

The application uses a weak algorithm, that is considered obsolete since it is relatively easy to break. These obsolete algorithms are vulnerable to several different kinds of attacks, including brute force.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.
- Do not use weak, outdated, or obsolete algorithms.
- Ensure you select the correct cryptographic mechanism according to the specific requirements.
- Passwords should be protected with a dedicated password protection scheme, such as bcrypt, scrypt, PBKDF2, or Argon2.

Specific Recommendations:

- Do not use SHA-1, MD5, or any other weak hash algorithm to protect passwords or personal data. Instead, use a stronger hash such as SHA-256 when a secure hash is required.
 - Do not use DES, Triple-DES, RC2, or any other weak encryption algorithm to protect passwords or personal data. Instead, use a stronger encryption algorithm such as AES to protect personal data.
 - Do not use weak encryption modes such as ECB, or rely on insecure defaults. Explicitly specify a stronger encryption mode, such as GCM.
 - For symmetric encryption, use a key length of at least 256 bits.
-

Source Code Examples

Java

Weakly Hashed PII

```
string protectSSN(HttpServletRequest req) {  
    string socialSecurityNum = req.getParameter("SocialSecurityNo");  
  
    return DigestUtils.md5Hex(socialSecurityNum);  
}
```

Stronger Hash for PII

```
string protectSSN(HttpServletRequest req) {  
    string socialSecurityNum = req.getParameter("SocialSecurityNo");  
  
    return DigestUtils.sha256Hex(socialSecurityNum);  
}
```

Use of a One Way Hash without a Salt

Risk

What might happen

If an attacker gains access to the hashed passwords, she would likely be able to reverse the hash due to this weakness, and retrieve the original password. Once the passwords are discovered, the attacker can impersonate the users, and take full advantage of their privileges and access their personal data. Furthermore, this would likely not be discovered, as the attacker is being identified solely by the victims' credentials.

Cause

How does it happen

Typical cryptographic hashes, such as SHA-1 and MD5, are incredibly fast. Combined with attack techniques such as precomputed Rainbow Tables, it is relatively easy for attackers to reverse the hashes, and discover the original passwords. Lack of a unique, random salt added to the password makes brute force attacks even simpler.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.
- Do not use weak, outdated, or obsolete algorithms.
- Ensure you select the correct cryptographic mechanism according to the specific requirements.

Specific Recommendations:

- Passwords should be protected using a password hashing algorithm, instead of a general cryptographic hash. This includes adaptive hashes such as bcrypt, scrypt, PBKDF2 and Argon2.
 - Tune the work factor, or cost, of the adaptive hash function according to the designated environment and risk profile.
 - Do not use a regular cryptographic hash, such as SHA-1 or MD5, to protect passwords, as these are too fast.
 - If it is necessary to use a common hash to protect passwords, add several bytes of unique, random data ("salt") to the password before hashing it. Store the salt with the hashed password, and do not reuse the same salt for multiple passwords.
-

Source Code Examples

Java

Unsalted Hashed Password

```
private String protectPassword(String password) {
```

```
byte[] data = password.getBytes();
byte[] hash = null;

MessageDigest md = MessageDigest.getInstance("MD5");
hash = md.digest(data);

return Base64.getEncoder().encodeToString(hash);
}
```

Fast Hash with Salt

```
private String protectPassword(String password) {
    byte[] data = password.getBytes("UTF-8");
    byte[] hash = null;

    try {
        MessageDigest md = MessageDigest.getInstance("SHA-1");

        SecureRandom rand = new SecureRandom();
        byte[] salt = new byte[32];
        rand.nextBytes(salt);

        md.update(salt);
        md.update(data);

        hash = md.digest();
    }
    catch (GeneralSecurityException gse) {
        handleCryptoErrors(gse);
    }
    finally {
        Arrays.fill(data, 0);
    }

    return Base64.getEncoder().encodeToString(hash);
}
```

Slow, Adaptive Password Hash

```
private String protectPassword(String password) {
    byte[] data = password.getBytes("UTF-8");
    byte[] hash = null;

    try {
        SecureRandom rand = new SecureRandom();
        byte[] salt = new byte[32];
        rand.nextBytes(salt);

        SecretKeyFactory skf = SecretKeyFactory.getInstance("PBKDF2WithHmacSHA512");
        PBEKeySpec spec = new PBEKeySpec(data, salt, ITERATION_COUNT, KEY_LENGTH);
        // ITERATION_COUNT should be configured by environment, KEY_LENGTH should be 256
        SecretKey key = skf.generateSecret(spec);

        hash = key.getEncoded();
    }
    catch (GeneralSecurityException gse) {
        handleCryptoErrors(gse);
    }
    finally {
        Arrays.fill(data, 0);
    }

    return Base64.getEncoder().encodeToString(hash);
}
```

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition `i=0` and the continuation condition `i<=2`, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
 - With array iterations, consider that arrays begin with cell 0 and end with cell `n-1`, for a size `n` array.
 - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
 - Where possible, use safe functions that manage memory and are not prone to off-by-one errors.
-

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
    ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
}
```

```
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
    ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf) -  
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

Potential Precision Problem

Risk

What might happen

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

Cause

How does it happen

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

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

General Recommendations

How to avoid it

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

Source Code Examples

Indicator of Poor Code Quality

Weakness ID: 398 (*Weakness Class*)

Status: Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|----------|------------------|-----|--|---|
| ChildOf | Category | 18 | Source Code | Development Concepts (primary)699 |
| ChildOf | Weakness Class | 710 | Coding Standards Violation | Research Concepts (primary)1000 |
| ParentOf | Weakness Variant | 107 | Struts: Unused Validation Form | Research Concepts (primary)1000 |
| ParentOf | Weakness Variant | 110 | Struts: Validator Without Form Field | Research Concepts (primary)1000 |
| ParentOf | Category | 399 | Resource Management Errors | Development Concepts (primary)699 |
| ParentOf | Weakness Base | 401 | Failure to Release Memory Before Removing Last Reference ('Memory Leak') | Seven Pernicious Kingdoms (primary)700 |
| ParentOf | Weakness Base | 404 | Improper Resource Shutdown or Release | Development Concepts699 Seven Pernicious Kingdoms (primary)700 |
| ParentOf | Weakness Variant | 415 | Double Free | Seven Pernicious Kingdoms (primary)700 |
| ParentOf | Weakness Base | 416 | Use After Free | Seven Pernicious Kingdoms (primary)700 |
| ParentOf | Weakness Variant | 457 | Use of Uninitialized Variable | Seven Pernicious Kingdoms (primary)700 |
| ParentOf | Weakness Base | 474 | Use of Function with Inconsistent Implementations | Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000 |
| ParentOf | Weakness Base | 475 | Undefined Behavior for Input to API | Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 |
| ParentOf | Weakness Base | 476 | NULL Pointer | Development |

| | | | | |
|----------|------------------|-----|--|--|
| | | | Dereference | Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000 |
| ParentOf | Weakness Base | 477 | Use of Obsolete Functions | Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000 |
| ParentOf | Weakness Variant | 478 | Missing Default Case in Switch Statement | Development Concepts (primary)699 |
| ParentOf | Weakness Variant | 479 | Unsafe Function Call from a Signal Handler | Development Concepts (primary)699 |
| ParentOf | Weakness Variant | 483 | Incorrect Block Delimitation | Development Concepts (primary)699 |
| ParentOf | Weakness Base | 484 | Omitted Break Statement in Switch | Development Concepts (primary)699 Research Concepts1000 |
| ParentOf | Weakness Variant | 546 | Suspicious Comment | Development Concepts (primary)699 Research Concepts (primary)1000 |
| ParentOf | Weakness Variant | 547 | Use of Hard-coded, Security-relevant Constants | Development Concepts (primary)699 Research Concepts (primary)1000 |
| ParentOf | Weakness Variant | 561 | Dead Code | Development Concepts (primary)699 Research Concepts (primary)1000 |
| ParentOf | Weakness Base | 562 | Return of Stack Variable Address | Development Concepts (primary)699 Research Concepts1000 |
| ParentOf | Weakness Variant | 563 | Unused Variable | Development Concepts (primary)699 Research Concepts (primary)1000 |
| ParentOf | Category | 569 | Expression Issues | Development Concepts (primary)699 |
| ParentOf | Weakness Variant | 585 | Empty Synchronized Block | Development Concepts (primary)699 Research Concepts (primary)1000 |
| ParentOf | Weakness Variant | 586 | Explicit Call to Finalize() | Development Concepts (primary)699 |
| ParentOf | Weakness Variant | 617 | Reachable Assertion | Development Concepts (primary)699 |
| ParentOf | Weakness Base | 676 | Use of Potentially Dangerous Function | Development Concepts (primary)699 Research Concepts (primary)1000 |
| MemberOf | View | 700 | Seven Pernicious Kingdoms | Seven Pernicious Kingdoms (primary)700 |

Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|----------------------|---------|-----|------------------|
|----------------------|---------|-----|------------------|

| | | | |
|-----------------------|--|--|--------------|
| 7 Pernicious Kingdoms | | | Code Quality |
|-----------------------|--|--|--------------|

Content History

Submissions

| Submission Date | Submitter | Organization | Source |
|-----------------|-----------------------|--------------|------------------|
| | 7 Pernicious Kingdoms | | Externally Mined |

Modifications

| Modification Date | Modifier | Organization | Source |
|-------------------|---|--------------|----------|
| 2008-07-01 | Eric Dalci updated Time of Introduction | Cigital | External |
| 2008-09-08 | CWE Content Team updated Description, Relationships, Taxonomy Mappings | MITRE | Internal |
| 2009-10-29 | CWE Content Team updated Relationships | MITRE | Internal |

Previous Entry Names

| Change Date | Previous Entry Name |
|-------------|---------------------|
| 2008-04-11 | Code Quality |

[BACK TO TOP](#)

Improper Access Control (Authorization)**Weakness ID:** 285 (*Weakness Class*)**Status:** Draft**Description****Description Summary**

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms**AuthZ:**

"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms**Languages**

Language-independent

Technology Classes

Web-Server: (*Often*)

Database-Server: (*Often*)

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

| Scope | Effect |
|-----------------|---|
| Confidentiality | An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data. |
| Integrity | An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data. |
| Integrity | An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality. |

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that `LookupMessageObject()` ensures that the `$id` argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: Perl

```
sub DisplayPrivateMessage {
my($id) = @_ ;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users. One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

| Reference | Description |
|-------------------------------|--|
| CVE-2009-3168 | Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords. |

| | |
|-------------------------------|---|
| CVE-2009-2960 | Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users. |
| CVE-2009-3597 | Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request. |
| CVE-2009-2282 | Terminal server does not check authorization for guest access. |
| CVE-2009-3230 | Database server does not use appropriate privileges for certain sensitive operations. |
| CVE-2009-2213 | Gateway uses default "Allow" configuration for its authorization settings. |
| CVE-2009-0034 | Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges. |
| CVE-2008-6123 | Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect. |
| CVE-2008-5027 | System monitoring software allows users to bypass authorization by creating custom forms. |
| CVE-2008-7109 | Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client. |
| CVE-2008-3424 | Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access. |
| CVE-2009-3781 | Content management system does not check access permissions for private files, allowing others to view those files. |
| CVE-2008-4577 | ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions. |
| CVE-2008-6548 | Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files. |
| CVE-2007-2925 | Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries. |
| CVE-2006-6679 | Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header. |
| CVE-2005-3623 | OS kernel does not check for a certain privilege before setting ACLs for files. |
| CVE-2005-2801 | Chain: file-system code performs an incorrect comparison (CWE-697), preventing defaults ACLs from being properly applied. |
| CVE-2001-1155 | Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions. |

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|----------|------------------|-----|---|--|
| ChildOf | Category | 254 | Security Features | Seven Pernicious Kingdoms (primary)700 |
| ChildOf | Weakness Class | 284 | Access Control (Authorization) Issues | Development Concepts (primary)699 Research Concepts (primary)1000 |
| ChildOf | Category | 721 | OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access | Weaknesses in OWASP Top Ten (2007) (primary)629 |
| ChildOf | Category | 723 | OWASP Top Ten 2004 Category A2 - Broken Access Control | Weaknesses in OWASP Top Ten (2004) (primary)711 |
| ChildOf | Category | 753 | 2009 Top 25 - Porous Defenses | Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750 |
| ChildOf | Category | 803 | 2010 Top 25 - Porous Defenses | Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800 |
| ParentOf | Weakness Variant | 219 | Sensitive Data Under Web Root | Research Concepts (primary)1000 |
| ParentOf | Weakness Base | 551 | Incorrect Behavior Order: Authorization Before Parsing and Canonicalization | Development Concepts (primary)699 Research Concepts1000 |
| ParentOf | Weakness Class | 638 | Failure to Use Complete Mediation | Research Concepts1000 |
| ParentOf | Weakness Base | 804 | Guessable CAPTCHA | Development Concepts (primary)699 Research Concepts (primary)1000 |

Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|-----------------------|---------|-------------------|--------------------------------|
| 7 Pernicious Kingdoms | | | Missing Access Control |
| OWASP Top Ten 2007 | A10 | CWE More Specific | Failure to Restrict URL Access |
| OWASP Top Ten 2004 | A2 | CWE More Specific | Broken Access Control |

Related Attack Patterns

| CAPEC-ID | Attack Pattern Name | (CAPEC Version: 1.5) |
|--------------------|--|----------------------|
| 1 | Accessing Functionality Not Properly Constrained by ACLs | |
| 13 | Subverting Environment Variable Values | |

| | |
|---------------------|---|
| 17 | Accessing, Modifying or Executing Executable Files |
| 87 | Forceful Browsing |
| 39 | Manipulating Opaque Client-based Data Tokens |
| 45 | Buffer Overflow via Symbolic Links |
| 51 | Poison Web Service Registry |
| 59 | Session Credential Falsification through Prediction |
| 60 | Reusing Session IDs (aka Session Replay) |
| 77 | Manipulating User-Controlled Variables |
| 76 | Manipulating Input to File System Calls |
| 104 | Cross Zone Scripting |

References

NIST. "Role Based Access Control and Role Based Security". <<http://csrc.nist.gov/groups/SNS/rbac/>>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

| Submissions | | | |
|----------------------|---|--------------|------------------|
| Submission Date | Submitter | Organization | Source |
| | 7 Pernicious Kingdoms | | Externally Mined |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Time of Introduction | | |
| 2008-08-15 | | Veracode | External |
| | Suggested OWASP Top Ten 2004 mapping | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Relationships, Other Notes, Taxonomy Mappings | | |
| 2009-01-12 | CWE Content Team | MITRE | Internal |
| | updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |
| | updated Potential Mitigations | | |
| 2009-05-27 | CWE Content Team | MITRE | Internal |
| | updated Description, Related Attack Patterns | | |
| 2009-07-27 | CWE Content Team | MITRE | Internal |
| | updated Relationships | | |
| 2009-10-29 | CWE Content Team | MITRE | Internal |
| | updated Type | | |
| 2009-12-28 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships | | |
| 2010-02-16 | CWE Content Team | MITRE | Internal |
| | updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships | | |
| 2010-04-05 | CWE Content Team | MITRE | Internal |
| | updated Potential Mitigations | | |
| Previous Entry Names | | | |
| Change Date | Previous Entry Name | | |
| 2009-01-12 | Missing or Inconsistent Access Control | | |

[BACK TO TOP](#)

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 (*Weakness Class*)

Status: Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

| Scope | Effect |
|-----------------|---|
| Confidentiality | An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file. |
| Integrity | An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse. |
| Availability | An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database. |

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: C

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
    fprintf(out, "hello world!\n");
    fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: Perl

```
$fileName = "secretFile.out";

if (-e $fileName) {
    chmod 0777, $fileName;
}
```

```
my $outFH;  
if (! open($outFH, ">>$fileName")) {  
    ExitError("Couldn't append to $fileName: $!");  
}  
my $dateString = FormatCurrentTime();  
my $status = IsHostAlive("cwe.mitre.org");  
print $outFH "$dateString cwe status: $status!\n";  
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: Shell

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

| Reference | Description |
|-------------------------------|---|
| CVE-2009-3482 | Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses. |
| CVE-2009-3897 | Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication. |
| CVE-2009-3489 | Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM. |
| CVE-2009-3289 | Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions. |
| CVE-2009-0115 | Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands. |
| CVE-2009-1073 | LDAP server stores a cleartext password in a world-readable file. |
| CVE-2009-0141 | Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users. |

| | |
|-------------------------------|--|
| CVE-2008-0662 | VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials. |
| CVE-2008-0322 | Driver installs its device interface with "Everyone: Write" permissions. |
| CVE-2009-3939 | Driver installs a file with world-writable permissions. |
| CVE-2009-3611 | Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups. |
| CVE-2007-6033 | Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution. |
| CVE-2007-5544 | Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session. |
| CVE-2005-4868 | Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials. |
| CVE-2004-1714 | Security product uses "Everyone: Full Control" permissions for its configuration files. |
| CVE-2001-0006 | "Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity. |
| CVE-2002-0969 | Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions. |

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|------------|-----------------------------|-----|--|--|
| ChildOf | Category | 275 | Permission Issues | Development Concepts (primary)699 |
| ChildOf | Weakness Class | 668 | Exposure of Resource to Wrong Sphere | Research Concepts (primary)1000 |
| ChildOf | Category | 753 | 2009 Top 25 - Porous Defenses | Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750 |
| ChildOf | Category | 803 | 2010 Top 25 - Porous Defenses | Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800 |
| RequiredBy | Compound Element: Composite | 689 | Permission Race Condition During Resource Copy | Research Concepts1000 |
| ParentOf | Weakness Variant | 276 | Incorrect Default Permissions | Research Concepts (primary)1000 |
| ParentOf | Weakness Variant | 277 | Insecure Inherited Permissions | Research Concepts (primary)1000 |
| ParentOf | Weakness Variant | 278 | Insecure Preserved Inherited Permissions | Research Concepts (primary)1000 |
| ParentOf | Weakness Variant | 279 | Incorrect Execution- Assigned Permissions | Research Concepts (primary)1000 |
| ParentOf | Weakness Base | 281 | Improper Preservation of Permissions | Research Concepts (primary)1000 |

Related Attack Patterns

| CAPEC-ID | Attack Pattern Name | (CAPEC Version: 1.5) |
|---------------------|--|----------------------|
| 232 | Exploitation of Privilege/Trust | |
| 1 | Accessing Functionality Not Properly Constrained by ACLs | |
| 17 | Accessing, Modifying or Executing Executable Files | |
| 60 | Reusing Session IDs (aka Session Replay) | |
| 61 | Session Fixation | |
| 62 | Cross Site Request Forgery (aka Session Riding) | |
| 122 | Exploitation of Authorization | |
| 180 | Exploiting Incorrectly Configured Access Control Security Levels | |
| 234 | Hijacking a privileged process | |

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

| Submissions | | | |
|----------------------|---|--------------|-------------------|
| Submission Date | Submitter | Organization | Source |
| 2008-09-08 | | | Internal CWE Team |
| | new weakness-focused entry for Research view. | | |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2009-01-12 | CWE Content Team | MITRE | Internal |
| | updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |
| | updated Potential Mitigations, Related Attack Patterns | | |
| 2009-05-27 | CWE Content Team | MITRE | Internal |
| | updated Name | | |
| 2009-12-28 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References | | |
| 2010-02-16 | CWE Content Team | MITRE | Internal |
| | updated Relationships | | |
| 2010-04-05 | CWE Content Team | MITRE | Internal |
| | updated Potential Mitigations, Related Attack Patterns | | |
| Previous Entry Names | | | |
| Change Date | Previous Entry Name | | |
| 2009-01-12 | Insecure Permission Assignment for Resource | | |
| 2009-05-27 | Insecure Permission Assignment for Critical Resource | | |

[BACK TO TOP](#)

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[...]
};
```

Information Leak Through Comments

Weakness ID: 615 (*Weakness Variant*)

Status: Incomplete

Description

Description Summary

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

Time of Introduction

Implementation

Demonstrative Examples

Example 1

The following comment, embedded in a JSP, will be displayed in the resulting HTML output.

(Bad Code)

Example Languages: **HTML and JSP**

```
<!-- FIXME: calling this with more than 30 args kills the JDBC server -->
```

Observed Examples

| Reference | Description |
|-------------------------------|---|
| CVE-2007-6197 | Version numbers and internal hostnames leaked in HTML comments. |
| CVE-2007-4072 | CMS places full pathname of server in HTML comment. |
| CVE-2009-2431 | blog software leaks real username in HTML comment. |

Potential Mitigations

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---------|------------------|-----|--------------------------------------|--|
| ChildOf | Weakness Variant | 540 | Information Leak Through Source Code | Development Concepts (primary)699 Research Concepts (primary)1000 |

Content History

| Submissions | | | |
|-------------------|---|--------------|------------------|
| Submission Date | Submitter | Organization | Source |
| | Anonymous Tool Vendor (under NDA) | | Externally Mined |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2008-07-01 | Sean Eidemiller | Cigital | External |
| | added/updated demonstrative examples | | |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Potential Mitigations, Time of Introduction | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Relationships, Taxonomy Mappings | | |
| 2008-10-14 | CWE Content Team | MITRE | Internal |
| | updated Description | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |

| | | | |
|------------|--|-------|----------|
| | updated Demonstrative Examples | | |
| 2009-07-27 | CWE Content Team | MITRE | Internal |
| | updated Observed Examples, Taxonomy Mappings | | |

[BACK TO TOP](#)

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.

Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredictable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.
-

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();  
  
long sessNum = random.nextLong();  
  
String sessionId = sessNum.toString();
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:@"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:@"%llu", sessBytes)
```

Privacy Violation

Risk

What might happen

A user's personal information could be stolen by a malicious programmer, or an attacker that intercepts the data.

Cause

How does it happen

The application sends user information, such as passwords, account information, or credit card numbers, outside the application, such as writing it to a local text or log file or sending it to an external web service.

General Recommendations

How to avoid it

1. Personal data should be removed before writing to logs or other files.
 2. Review the need and justification of sending personal data to remote web services.
-

Source Code Examples

CSharp

The user's password is written to the screen

```
class PrivacyViolation
{
    static void foo(string insert_sql)
    {
        string password = "unsafe_password";
        insert_sql = insert_sql.Replace("$password", password);
        System.Console.WriteLine(insert_sql);
    }
}
```

the user's password is MD5 coded before being written to the screen

```
class PrivacyViolationFixed
{
    static void foo(string insert_sql)
    {
```

```
        string password = "unsafe_password";
        MD5 md5Hash = System.Security.Cryptography.MD5.Create();
        byte[] data = md5Hash.ComputeHash(Encoding.UTF8.GetBytes(password));
        StringBuilder md5Password = new StringBuilder();

        for (int i = 0; i < data.Length; i++)
        {
            md5Password.Append(data[i].ToString("x2"));
        }
        insert_sql = insert_sql.Replace("$password", md5Password.ToString());
        System.Console.WriteLine(insert_sql);
    }
}
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this function. These functions often return error codes in the result, or share other status codes with its caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.
 - Ensure the calling function responds to all possible return values.
 - Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.
-

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 (*Weakness Variant*)

Status: Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

| Scope | Effect |
|-----------|---|
| Integrity | This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows. |

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: C and C++

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: C and C++

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

/ Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */*

```
char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strcmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strcmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In `AuthenticateUser()`, because `sizeof()` is applied to a parameter with an array type, the `sizeof()` call might return 4 on many modern architectures. As a result, the `strcmp()` call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "`sizeof(*pointer)`" instead of "`sizeof(pointer)`", unless you intend to run `sizeof()` on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of `sizeof()` on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of `sizeof(pointer)` indicates a bug.

Weakness Ordinalities

| Ordinality | Description |
|------------|---|
| Primary | (where the weakness exists independent of other weaknesses) |

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|------------|----------------|-----|---|---|
| ChildOf | Category | 465 | Pointer Issues | Development Concepts (primary)699 |
| ChildOf | Weakness Class | 682 | Incorrect Calculation | Research Concepts (primary)1000 |
| ChildOf | Category | 737 | CERT C Secure Coding Section 03 - Expressions (EXP) | Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734 |
| ChildOf | Category | 740 | CERT C Secure Coding Section 06 - Arrays (ARR) | Weaknesses Addressed by the CERT C Secure Coding Standard734 |
| CanPrecede | Weakness Base | 131 | Incorrect Calculation of Buffer Size | Research Concepts1000 |

Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|----------------------|---------|-----|--|
| CLASP | | | Use of sizeof() on a pointer type |
| CERT C Secure Coding | ARR01-C | | Do not apply the sizeof operator to a pointer when taking the size of an array |
| CERT C Secure Coding | EXP01-C | | Do not take the size of a pointer to determine the size of the pointed-to type |

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type".
<https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

| Submissions | | | |
|-------------------|---|---------------|------------------|
| Submission Date | Submitter | Organization | Source |
| | CLASP | | Externally Mined |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Time of Introduction | | |
| 2008-08-01 | | KDM Analytics | External |
| | added/updated white box definitions | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities | | |
| 2008-11-24 | CWE Content Team | MITRE | Internal |
| | updated Relationships, Taxonomy Mappings | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |
| 2009-12-28 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |
| 2010-02-16 | CWE Content Team | MITRE | Internal |
| | updated Relationships | | |

[BACK TO TOP](#)

Reliance on DNS Lookups in a Decision

Risk

What might happen

Relying on reverse DNS records, without verifying domain ownership via cryptographic certificates or protocols, is not a sufficient authentication mechanism. Basing any security decisions on the registered hostname could allow an external attacker to control the application flow. The attacker could possibly perform restricted operations, bypass access controls, and even spoof the user's identity, inject a bogus hostname into the security log, and possibly other logic attacks.

Cause

How does it happen

The application performs a reverse DNS resolution, based on the remote IP address, and performs a security check based on the returned hostname. However, it is relatively easy to spoof DNS names, or cause them to be misreported, depending on the context of the specific environment. If the remote server is controlled by the attacker, it can be configured to report a bogus hostname. Additionally, the attacker could also spoof the hostname if she controls the associated DNS server, or by attacking the legitimate DNS server, or by poisoning the server's DNS cache, or by modifying unprotected DNS traffic to the server. Regardless of the vector, a remote attacker can alter the detected network address, faking the authentication details.

General Recommendations

How to avoid it

- Do not rely on DNS records, network addresses, or system hostnames as a form of authentication, or any other security-related decision.
 - Do not perform reverse DNS resolution over an unprotected protocol without record validation.
 - Implement a proper authentication mechanism, such as passwords, cryptographic certificates, or public key digital signatures.
 - Consider using proposed protocol extensions to cryptographically protect DNS, e.g. DNSSEC (though note the limited support and other drawbacks).
-

Source Code Examples

Java

Using Reverse DNS as Authentication

```
private boolean isInternalEmployee(ServletRequest req) {
    boolean isCompany = false;

    String ip = req.getRemoteAddr();
    InetAddress address = InetAddress.getByName(ip);

    if (address.getHostName().endsWith(COMPANYNAME)) {
        isCompany = true;
    }

    return isCompany;
}
```

```
}
```

Verify Authenticated User's Identity

```
private boolean isInternalEmployee(HttpServletRequest req) {  
    boolean isCompany = false;  
  
    Principal user = req.getUserPrincipal();  
    if (user != null) {  
        if (user.getName().startsWith(COMPANYDOMAIN + "\\\")) {  
            isCompany = true;  
        }  
    }  
    return isCompany;  
}
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
 - Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
 - Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.
-

Source Code Examples

Use of sizeof() on a Pointer Type

Weakness ID: 467 (*Weakness Variant*)

Status: Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

| Scope | Effect |
|-----------|---|
| Integrity | This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows. |

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(*Bad Code*)

Example Languages: C and C++

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(*Good Code*)

Example Languages: C and C++

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(*Bad Code*)

/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

```
char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strcmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strcmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In `AuthenticateUser()`, because `sizeof()` is applied to a parameter with an array type, the `sizeof()` call might return 4 on many modern architectures. As a result, the `strcmp()` call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "`sizeof(*pointer)`" instead of "`sizeof(pointer)`", unless you intend to run `sizeof()` on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of `sizeof()` on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of `sizeof(pointer)` indicates a bug.

Weakness Ordinalities

| Ordinality | Description |
|------------|---|
| Primary | (where the weakness exists independent of other weaknesses) |

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|------------|----------------|-----|---|---|
| ChildOf | Category | 465 | Pointer Issues | Development Concepts (primary)699 |
| ChildOf | Weakness Class | 682 | Incorrect Calculation | Research Concepts (primary)1000 |
| ChildOf | Category | 737 | CERT C Secure Coding Section 03 - Expressions (EXP) | Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734 |
| ChildOf | Category | 740 | CERT C Secure Coding Section 06 - Arrays (ARR) | Weaknesses Addressed by the CERT C Secure Coding Standard734 |
| CanPrecede | Weakness Base | 131 | Incorrect Calculation of Buffer Size | Research Concepts1000 |

Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|----------------------|---------|-----|--|
| CLASP | | | Use of sizeof() on a pointer type |
| CERT C Secure Coding | ARR01-C | | Do not apply the sizeof operator to a pointer when taking the size of an array |
| CERT C Secure Coding | EXP01-C | | Do not take the size of a pointer to determine the size of the pointed-to type |

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type".
<https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

| Submissions | | | |
|-------------------|---|---------------|------------------|
| Submission Date | Submitter | Organization | Source |
| | CLASP | | Externally Mined |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Time of Introduction | | |
| 2008-08-01 | | KDM Analytics | External |
| | added/updated white box definitions | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities | | |
| 2008-11-24 | CWE Content Team | MITRE | Internal |
| | updated Relationships, Taxonomy Mappings | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |
| 2009-12-28 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |
| 2010-02-16 | CWE Content Team | MITRE | Internal |
| | updated Relationships | | |

[BACK TO TOP](#)

Improper Validation of Array Index

Weakness ID: 129 (*Weakness Base*)

Status: Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

Implementation

Applicable Platforms

Languages

C: (*Often*)

C++: (*Often*)

Language-independent

Common Consequences

| Scope | Effect |
|--|--|
| Integrity Availability | Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area. |
| Integrity | If the memory corrupted is data, rather than instructions, the system will continue to function with improper values. |
| Confidentiality Integrity | Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data. |
| Integrity | If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled. |
| Integrity Availability Confidentiality | A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution. |

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: C

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
    ...
    char buf[BUFFER_SIZE];
    int ok;
    int num, size;

    // read values from socket and added to sizes array
    while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
    {

        // continue read from socket until buf only contains '.'
        if (DOTLINE(buf))
            break;
        else if (sscanf(buf, "%d %d", &num, &size) == 2)
            sizes[num - 1] = size;
        }
    ...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: C

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
    ...
    char buf[BUFFER_SIZE];
    int ok;
    int num, size;

    // read values from socket and added to sizes array
    while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
    {

        // continue read from socket until buf only contains '.'
        if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: Java

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an `ArrayIndexOutOfBoundsException` Exception being raised.

Example 3

In the following Java example the method `displayProductSummary` is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the `displayProductSummary` method. The `displayProductSummary` method passes the integer value of the product number to the `getProductSummary` method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: Java

// Method called from servlet to obtain product information

```
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may cause the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: Java

// Method called from servlet to obtain product information

```
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as `ArrayList` that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: Java

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

| Reference | Description |
|-------------------------------|---|
| CVE-2005-0369 | large ID in packet used as array index |
| CVE-2001-1009 | negative array index as argument to POP LIST command |
| CVE-2003-0721 | Integer signedness error leads to negative array index |
| CVE-2004-1189 | product does not properly track a count and a maximum number, which can lead to resultant array index overflow. |
| CVE-2007-5756 | chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error. |

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

| Ordinality | Description |
|------------|--|
| Resultant | The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer. |

Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|------------|------------------|-----|--|--|
| ChildOf | Weakness Class | 20 | Improper Input Validation | Development Concepts (primary)699 Research Concepts (primary)1000 |
| ChildOf | Category | 189 | Numeric Errors | Development Concepts699 |
| ChildOf | Category | 633 | Weaknesses that Affect Memory | Resource-specific Weaknesses (primary)631 |
| ChildOf | Category | 738 | CERT C Secure Coding Section 04 - Integers (INT) | Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734 |
| ChildOf | Category | 740 | CERT C Secure Coding Section 06 - Arrays (ARR) | Weaknesses Addressed by the CERT C Secure Coding Standard734 |
| ChildOf | Category | 802 | 2010 Top 25 - Risky Resource Management | Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800 |
| CanPrecede | Weakness Class | 119 | Failure to Constrain Operations within the Bounds of a Memory Buffer | Research Concepts1000 |
| CanPrecede | Weakness Variant | 789 | Uncontrolled Memory Allocation | Research Concepts1000 |
| PeerOf | Weakness Base | 124 | Buffer Underwrite ('Buffer Underflow') | Research Concepts1000 |

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

Memory

f Causal Nature

Explicit

Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|----------------------|---------|-----|---|
| CLASP | | | Unchecked array indexing |
| PLOVER | | | INDEX - Array index overflow |
| CERT C Secure Coding | ARR00-C | | Understand how arrays work |
| CERT C Secure Coding | ARR30-C | | Guarantee that array indices are within the valid range |
| CERT C Secure Coding | ARR38-C | | Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element |
| CERT C Secure Coding | INT32-C | | Ensure that operations on signed integers do not result in overflow |

Related Attack Patterns

| CAPEC-ID | Attack Pattern Name | (CAPEC Version: 1.5) |
|---------------------|---------------------|----------------------|
| 100 | Overflow Buffers | |

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

| Submissions | | | |
|----------------------|---|--------------|------------------|
| Submission Date | Submitter | Organization | Source |
| | CLASP | | Externally Mined |
| Modifications | | | |
| Modification Date | Modifier | Organization | Source |
| 2008-07-01 | Sean Eidemiller | Cigital | External |
| | added/updated demonstrative examples | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities | | |
| 2008-11-24 | CWE Content Team | MITRE | Internal |
| | updated Relationships, Taxonomy Mappings | | |
| 2009-01-12 | CWE Content Team | MITRE | Internal |
| | updated Common Consequences | | |
| 2009-10-29 | CWE Content Team | MITRE | Internal |
| | updated Description, Name, Relationships | | |
| 2009-12-28 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities | | |
| 2010-02-16 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships | | |
| 2010-04-05 | CWE Content Team | MITRE | Internal |
| | updated Related Attack Patterns | | |
| Previous Entry Names | | | |
| Change Date | Previous Entry Name | | |
| 2009-10-29 | Unchecked Array Indexing | | |

[BACK TO TOP](#)

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overridden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
public static int counter = 0;
public static void start() throws InterruptedException {
    incrementCounter ic;
    decrementCounter dc;
    while(counter == 0) {
        counter = 0;
        ic = new incrementCounter();
        dc = new decrementCounter();
        ic.start();
        dc.start();
        ic.join();
        dc.join();
    }
    System.out.println(counter); //Will stop and return either -1 or 1 due to race
    condition over counter
}

public static class incrementCounter extends Thread {
    public void run() {
        counter++;
    }
}
```

```
}

public static class decrementCounter extends Thread {
    public void run() {
        counter--;
    }
}
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
public static int counter = 0;
public static Object lock = new Object();

public static void start() throws InterruptedException {
    incrementCounter ic;
    decrementCounter dc;
    while(counter == 0) { // because of proper locking, this condition is never false
        counter = 0;
        ic = new incrementCounter();
        dc = new decrementCounter();
        ic.start();
        dc.start();
        ic.join();
        dc.join();
    }
    System.out.println(counter); // Never reached
}

public static class incrementCounter extends Thread {
    public void run() {
        synchronized (lock) {
            counter++;
        }
    }
}

public static class decrementCounter extends Thread {
    public void run() {
        synchronized (lock) {
            counter--;
        }
    }
}
```

Scanned Languages

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