CloverBootloader Scan Report

Project Name	CloverBootloader
Scan Start	Friday, June 21, 2024 1:26:30 PM
Preset	Checkmarx Default
Scan Time	01h:20m:06s
Lines Of Code Scanned	105442
Files Scanned	78
Report Creation Time	Friday, June 21, 2024 2:54:57 PM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	4/1000 (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

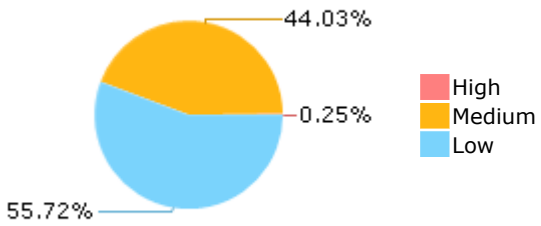
Results Limit

Results limit per query was set to 50

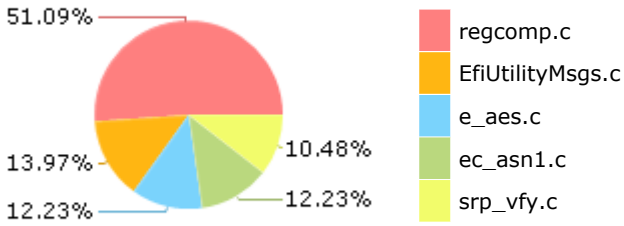
Selected Queries

Selected queries are listed in Result Summary

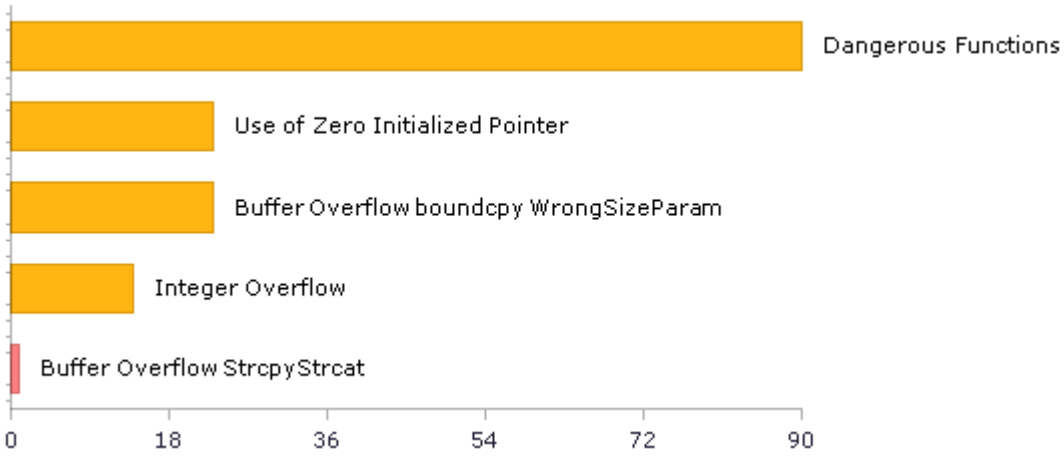
Result Summary



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	110	54
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	123	123
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	2	2
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	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	90	90
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2013

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	2	2
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	90	90
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	3	3
PCI DSS (3.2) - 6.5.2 - Buffer overflows	45	43
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	0	0
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	2	2
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.	124	124
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.	3	3
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.	16	16

***** 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)	125	125
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	1	1
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	1	1
SC-4 Information in Shared Resources (P1)	2	2
SC-5 Denial of Service Protection (P1)*	117	45
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	26	24
SI-11 Error Handling (P2)*	4	4
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	3	3

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

Scan Summary - OWASP Mobile Top 10 2016

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

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

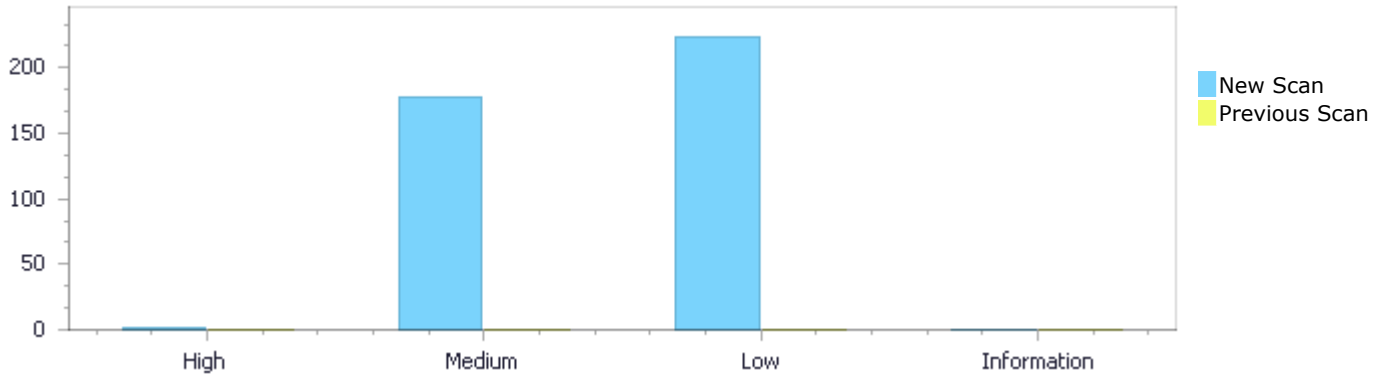
Scan Summary - Custom

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

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	1	177	224	0	402
Recurrent Issues	0	0	0	0	0
Total	1	177	224	0	402
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	1	177	224	0	402
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	1	177	224	0	402

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	1	High
Dangerous Functions	90	Medium
Buffer Overflow boundcpy WrongSizeParam	23	Medium
Use of Zero Initialized Pointer	23	Medium
Integer Overflow	14	Medium

Use of Uninitialized Pointer	13	Medium
Wrong Size t Allocation	5	Medium
Heap Inspection	2	Medium
Long Overflow	2	Medium
Buffer Overflow AddressOfLocalVarReturned	1	Medium
Char Overflow	1	Medium
Divide By Zero	1	Medium
Memory Leak	1	Medium
Use of a One Way Hash without a Salt	1	Medium
Improper Resource Access Authorization	123	Low
NULL Pointer Dereference	79	Low
Unchecked Array Index	5	Low
Unchecked Return Value	4	Low
Heuristic 2nd Order Buffer Overflow read	3	Low
Potential Off by One Error in Loops	3	Low
Exposure of System Data to Unauthorized Control Sphere	2	Low
Sizeof Pointer Argument	2	Low
Inconsistent Implementations	1	Low
Information Exposure Through Comments	1	Low
TOCTOU	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
CloverBootloader/e_aes.c	22
CloverBootloader/EfiUtilityMsgs.c	22
CloverBootloader/tasn_enc.c	18
CloverBootloader/evp_enc.c	13
CloverBootloader/a_object.c	12
CloverBootloader/a_bytes.c	10
CloverBootloader/e_aes_cbc_hmac_sha1.c	10
CloverBootloader/regcomp.c	6
CloverBootloader/a_int.c	6
CloverBootloader/srp_vfy.c	6

Scan Results Details

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=1020030&projectid=20025&pathid=1
Status	New

The size of the buffer used by *CRYPTO_strdup in ret, at line 460 of CloverBootloader/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 460 of CloverBootloader/mem.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/mem.c	CloverBootloader/mem.c
Line	460	464
Object	file	ret

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

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

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=1020030&projectid=20025&pathid=146
Status	New

The dangerous function, memcpy, was found in use at line 252 in CloverBootloader/a_bytes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	295	295
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/a_bytes.c
Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

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

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=147
Status	New

The dangerous function, memcpy, was found in use at line 66 in CloverBootloader/a_bytes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	110	110
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/a_bytes.c
Method ASN1_STRING *d2i_ASN1_type_bytes(ASN1_STRING **a, const unsigned char **pp,

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

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=148

Status	New

The dangerous function, memcpy, was found in use at line 131 in CloverBootloader/a_bytes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	151	151
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/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 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=149
Status	New

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

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	222	222
Object	memcpy	memcpy

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

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

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=150
Status	New

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

	Source	Destination
File	CloverBootloader/a_int.c	CloverBootloader/a_int.c
Line	153	153
Object	memcpy	memcpy

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

```
....
153.        else if (!neg) memcpy(p,a->data,(unsigned int)a->length);
```

Dangerous Functions\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=151
Status New

The dangerous function, memcpy, was found in use at line 178 in CloverBootloader/a_int.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/a_int.c	CloverBootloader/a_int.c
Line	249	249
Object	memcpy	memcpy

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

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

Dangerous Functions\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=152
Status New

The dangerous function, memcpy, was found in use at line 271 in CloverBootloader/a_int.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/a_int.c	CloverBootloader/a_int.c
Line	318	318
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/a_int.c
Method ASN1_INTEGER *d2i_ASN1_UINTEGER(ASN1_INTEGER **a, const unsigned char **pp,

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

Dangerous Functions\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=153
Status New

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

	Source	Destination
File	CloverBootloader/a_object.c	CloverBootloader/a_object.c
Line	79	79
Object	memcpy	memcpy

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

```
....
79.    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=1020030&projectid=20025&pathid=154
Status New

The dangerous function, memcpy, was found in use at line 286 in CloverBootloader/a_object.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	CloverBootloader/a_object.c	CloverBootloader/a_object.c
Line	328	328
Object	memcpy	memcpy

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

```
....
328.         memcpy(data,p,(int)len);
```

Dangerous Functions\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=155
Status New

The dangerous function, memcpy, was found in use at line 726 in CloverBootloader/b_print.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/b_print.c	CloverBootloader/b_print.c
Line	744	744
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/b_print.c
Method doapr_outch(

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

Dangerous Functions\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=156
Status New

The dangerous function, memcpy, was found in use at line 239 in CloverBootloader/cms_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/cms_enc.c	CloverBootloader/cms_enc.c

Line	249	249
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/cms_enc.c
Method int cms_EncryptedContent_init(CMS_EncryptedContentInfo *ec,

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

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=157
Status	New

The dangerous function, memcpy, was found in use at line 224 in CloverBootloader/cms_pwri.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/cms_pwri.c	CloverBootloader/cms_pwri.c
Line	269	269
Object	memcpy	memcpy

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

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

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=158
Status	New

The dangerous function, memcpy, was found in use at line 278 in CloverBootloader/cms_pwri.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/cms_pwri.c	CloverBootloader/cms_pwri.c
Line	306	306
Object	memcpy	memcpy

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

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

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=159
Status	New

The dangerous function, memcpy, was found in use at line 291 in CloverBootloader/digest.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/digest.c	CloverBootloader/digest.c
Line	315	315
Object	memcpy	memcpy

Code Snippet	
File Name	CloverBootloader/digest.c
Method	int EVP_MD_CTX_copy_ex(EVP_MD_CTX *out, const EVP_MD_CTX *in)

```
....
315.        memcpy(out,in,sizeof *out);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=160
Status	New

The dangerous function, memcpy, was found in use at line 291 in CloverBootloader/digest.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/digest.c	CloverBootloader/digest.c
Line	330	330
Object	memcpy	memcpy

Code Snippet	
File Name	CloverBootloader/digest.c

Method	int EVP_MD_CTX_copy_ex(EVP_MD_CTX *out, const EVP_MD_CTX *in)

```
....
330.              memcpy(out->md_data,in->md_data,out->digest-
>ctx_size);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=161
Status	New

The dangerous function, memcpy, was found in use at line 305 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	335	335
Object	memcpy	memcpy

Code Snippet	
File Name	CloverBootloader/e_aes.c
Method	static int aesni_gcm_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
335.                    memcpy(gctx->iv, iv, gctx->ivlen);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=162
Status	New

The dangerous function, memcpy, was found in use at line 346 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	379	379
Object	memcpy	memcpy

Code Snippet	
File Name	CloverBootloader/e_aes.c
Method	static int aesni_xts_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
379.              memcpy(ctx->iv, iv, 16);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=163
Status	New

The dangerous function, memcpy, was found in use at line 389 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	406	406
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aesni_ccm_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
406.              memcpy(ctx->iv, iv, 15 - cctx->L);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=164
Status	New

The dangerous function, memcpy, was found in use at line 700 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	738	738
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
738.              memcpy(c->buf, ptr, arg);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=165
Status	New

The dangerous function, memcpy, was found in use at line 700 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	745	745
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
745.              memcpy(ptr, c->buf, arg);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=166
Status	New

The dangerous function, memcpy, was found in use at line 700 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	752	752
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
752.                    memcpy(gctx->iv, ptr, gctx->ivlen);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=167
Status	New

The dangerous function, memcpy, was found in use at line 700 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	762	762
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
762.                    memcpy(gctx->iv, ptr, arg);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=168
Status	New

The dangerous function, memcpy, was found in use at line 700 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	775	775
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
775.              memcpy(ptr, gctx->iv + gctx->ivlen - arg, arg);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=169
Status	New

The dangerous function, memcpy, was found in use at line 700 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	787	787
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
787.              memcpy(gctx->iv + gctx->ivlen - arg, ptr, arg);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=170
Status	New

The dangerous function, memcpy, was found in use at line 700 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	796	796
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
796.              memcpy(c->buf, ptr, arg);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=171
Status	New

The dangerous function, memcpy, was found in use at line 817 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	873	873
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
873.                    memcpy(gctx->iv, iv, gctx->ivlen);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=172
Status	New

The dangerous function, memcpy, was found in use at line 1052 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	1115	1115
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_xts_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
1115.              memcpy(ctx->iv, iv, 16);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=173
Status	New

The dangerous function, memcpy, was found in use at line 1155 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	1185	1185
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_ccm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
1185.                    memcpy(c->buf, ptr, arg);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=174
Status	New

The dangerous function, memcpy, was found in use at line 1206 in CloverBootloader/e_aes.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	1233	1233
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_ccm_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
1233.             memcpy(ctx->iv, iv, 15 - cctx->L);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=175
Status	New

The dangerous function, memcpy, was found in use at line 179 in CloverBootloader/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes_cbc_hmac_sha1.c	CloverBootloader/e_aes_cbc_hmac_sha1.c
Line	227	227
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
227.                          memcpy(out+aes_off,in+aes_off,plen-
aes_off);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=176
Status	New

The dangerous function, memcpy, was found in use at line 456 in CloverBootloader/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes_cbc_hmac_sha1.c	CloverBootloader/e_aes_cbc_hmac_sha1.c
Line	474	474
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/e_aes_cbc_hmac_sha1.c

Method	static int aesni_cbc_hmac_sha1_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg, void *ptr)

```
....
474.                    memcpy(hmac_key,ptr,arg);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=177
Status	New

The dangerous function, memcpy, was found in use at line 456 in CloverBootloader/e_aes_cbc_hmac_sha1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_aes_cbc_hmac_sha1.c	CloverBootloader/e_aes_cbc_hmac_sha1.c
Line	513	513
Object	memcpy	memcpy

Code Snippet	
File Name	CloverBootloader/e_aes_cbc_hmac_sha1.c
Method	static int aesni_cbc_hmac_sha1_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg, void *ptr)

```
....
513.                    memcpy(key->aux.tls_aad,ptr,arg);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=178
Status	New

The dangerous function, memcpy, was found in use at line 116 in CloverBootloader/e_rc4_hmac_md5.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_rc4_hmac_md5.c	CloverBootloader/e_rc4_hmac_md5.c
Line	159	159
Object	memcpy	memcpy

Code Snippet	
File Name	CloverBootloader/e_rc4_hmac_md5.c

Method	static int rc4_hmac_md5_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
159.                            memcpy(out+rc4_off,in+rc4_off,plen-
rc4_off);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=179
Status	New

The dangerous function, memcpy, was found in use at line 220 in CloverBootloader/e_rc4_hmac_md5.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/e_rc4_hmac_md5.c	CloverBootloader/e_rc4_hmac_md5.c
Line	238	238
Object	memcpy	memcpy

Code Snippet	
File Name	CloverBootloader/e_rc4_hmac_md5.c
Method	static int rc4_hmac_md5_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg, void *ptr)

```
....
238.                        memcpy(hmac_key,ptr,arg);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=180
Status	New

The dangerous function, memcpy, was found in use at line 747 in CloverBootloader/ec_asn1.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/ec_asn1.c	CloverBootloader/ec_asn1.c
Line	933	933
Object	memcpy	memcpy

Code Snippet	
File Name	CloverBootloader/ec_asn1.c
Method	static EC_GROUP *ec_asn1_parameters2group(const ECPARAMETERS *params)

```
....
933.              memcpy(ret->seed, params->curve->seed->data,
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=181
Status	New

The dangerous function, memcpy, was found in use at line 108 in CloverBootloader/ech_ossl.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/ech_ossl.c	CloverBootloader/ech_ossl.c
Line	205	205
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/ech_ossl.c
Method static int ecdh_compute_key(void *out, size_t outlen, const EC_POINT *pub_key,

```
....
205.              memcpy(out, buf, outlen);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=182
Status	New

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

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	664	664
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/evp_enc.c
Method int EVP_CIPHER_CTX_copy(EVP_CIPHER_CTX *out, const EVP_CIPHER_CTX *in)

```
....
664.        memcpy(out,in,sizeof *out);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=183
Status	New

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

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	674	674
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/evp_enc.c
Method int EVP_CIPHER_CTX_copy(EVP_CIPHER_CTX *out, const EVP_CIPHER_CTX *in)

```
....
674.              memcpy(out->cipher_data,in->cipher_data,in->cipher-
>ctx_size);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=184
Status	New

The dangerous function, memcpy, was found in use at line 103 in CloverBootloader/evp_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	235	235
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/evp_enc.c
Method int EVP_CipherInit_ex(EVP_CIPHER_CTX *ctx, const EVP_CIPHER *cipher, ENGINE *impl,

```
....
235.                    if(iv) memcpy(ctx->oiv, iv,
EVP_CIPHER_CTX_iv_length(ctx));
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=185
Status	New

The dangerous function, memcpy, was found in use at line 103 in CloverBootloader/evp_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	236	236
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/evp_enc.c
Method int EVP_CipherInit_ex(EVP_CIPHER_CTX *ctx, const EVP_CIPHER *cipher, ENGINE *impl,

```
....
236.                    memcpy(ctx->iv, ctx->oiv,
EVP_CIPHER_CTX_iv_length(ctx));
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=186
Status	New

The dangerous function, memcpy, was found in use at line 103 in CloverBootloader/evp_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	243	243
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/evp_enc.c

Method	int EVP_CipherInit_ex(EVP_CIPHER_CTX *ctx, const EVP_CIPHER *cipher, ENGINE *impl,

```
....
243.                            memcpy(ctx->iv, iv,
EVP_CIPHER_CTX_iv_length(ctx));
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=187
Status	New

The dangerous function, memcpy, was found in use at line 307 in CloverBootloader/evp_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	348	348
Object	memcpy	memcpy

Code Snippet	
File Name	CloverBootloader/evp_enc.c
Method	int EVP_EncryptUpdate(EVP_CIPHER_CTX *ctx, unsigned char *out, int *outl,

```
....
348.                    memcpy(&(ctx->buf[i]),in,inl);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=188
Status	New

The dangerous function, memcpy, was found in use at line 307 in CloverBootloader/evp_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	356	356
Object	memcpy	memcpy

Code Snippet	
File Name	CloverBootloader/evp_enc.c
Method	int EVP_EncryptUpdate(EVP_CIPHER_CTX *ctx, unsigned char *out, int *outl,

```
....
356.                    memcpy(&(ctx->buf[i]),in,j);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=189
Status	New

The dangerous function, memcpy, was found in use at line 307 in CloverBootloader/evp_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	375	375
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/evp_enc.c
Method int EVP_EncryptUpdate(EVP_CIPHER_CTX *ctx, unsigned char *out, int *outl,

```
....
375.                memcpy(ctx->buf,&(in[inl]),i);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=190
Status	New

The dangerous function, memcpy, was found in use at line 433 in CloverBootloader/evp_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	466	466
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/evp_enc.c
Method int EVP_DecryptUpdate(EVP_CIPHER_CTX *ctx, unsigned char *out, int *outl,

```
....
466.                memcpy(out,ctx->final,b);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=191
Status	New

The dangerous function, memcpy, was found in use at line 433 in CloverBootloader/evp_enc.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	483	483
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/evp_enc.c
Method int EVP_DecryptUpdate(EVP_CIPHER_CTX *ctx, unsigned char *out, int *outl,

```
....
483.                memcpy(ctx->final,&out[*outl],b);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=192
Status	New

The dangerous function, memcpy, was found in use at line 489 in CloverBootloader/mem.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/mem.c	CloverBootloader/mem.c
Line	508	508
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/mem.c
Method void *CRYPTO_realloc_clean(void *str, int old_len, int num, const char *file,

```
....
508.                memcpy(ret,str,old_len);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=193
Status	New

The dangerous function, memcpy, was found in use at line 154 in CloverBootloader/rsa_sign.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/rsa_sign.c	CloverBootloader/rsa_sign.c
Line	209	209
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/rsa_sign.c
Method int int_rsa_verify(int dtype, const unsigned char *m,

```
....
209.                    memcpy(rm, s + 2, 16);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=194
Status	New

The dangerous function, memcpy, was found in use at line 154 in CloverBootloader/rsa_sign.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/rsa_sign.c	CloverBootloader/rsa_sign.c
Line	282	282
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/rsa_sign.c
Method int int_rsa_verify(int dtype, const unsigned char *m,

```
....
282.                        memcpy(rm, sig->digest->data,
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=195
Status	New

The dangerous function, memcpy, was found in use at line 1220 in CloverBootloader/tasn_dec.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	CloverBootloader/tasn_dec.c	CloverBootloader/tasn_dec.c
Line	1231	1231
Object	memcpy	memcpy

Code Snippet
File Name CloverBootloader/tasn_dec.c
Method static int collect_data(BUF_MEM *buf, const unsigned char **p, long plen)

```
....
1231.             memcpy(buf->data + len, *p, plen);
```

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=1020030&projectid=20025&pathid=12
Status	New

The size of the buffer used by EVP_CIPHER_CTX_init in EVP_CIPHER_CTX, at line 81 of CloverBootloader/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 81 of CloverBootloader/evp_enc.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c

Line	83	83
Object	EVP_CIPHER_CTX	EVP_CIPHER_CTX

Code Snippet
File Name CloverBootloader/evp_enc.c
Method void EVP_CIPHER_CTX_init(EVP_CIPHER_CTX *ctx)

```
....
83.    memset(ctx,0,sizeof(EVP_CIPHER_CTX));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=13
Status	New

The size of the buffer used by EVP_CIPHER_CTX_cleanup in EVP_CIPHER_CTX, at line 569 of CloverBootloader/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 569 of CloverBootloader/evp_enc.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	592	592
Object	EVP_CIPHER_CTX	EVP_CIPHER_CTX

Code Snippet
File Name CloverBootloader/evp_enc.c
Method int EVP_CIPHER_CTX_cleanup(EVP_CIPHER_CTX *c)

```
....
592.        memset(c,0,sizeof(EVP_CIPHER_CTX));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=14
Status	New

The size of the buffer used by ASN1_INTEGER_set in long, at line 335 of CloverBootloader/a_int.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ASN1_INTEGER_set passes to long, at line 335 of CloverBootloader/a_int.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/a_int.c	CloverBootloader/a_int.c

Line	348	348
Object	long	long

Code Snippet
File Name CloverBootloader/a_int.c
Method int ASN1_INTEGER_set(ASN1_INTEGER *a, long v)

```
....
348.                    memset((char *)a->data,0,sizeof(long)+1);
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=15
Status	New

The size of the buffer used by asn1_collate_primitive in os, at line 252 of CloverBootloader/a_bytes.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that asn1_collate_primitive passes to os, at line 252 of CloverBootloader/a_bytes.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	295	295
Object	os	os

Code Snippet
File Name CloverBootloader/a_bytes.c
Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

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

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=16
Status	New

The size of the buffer used by i2d_ASN1_bytes in a, at line 131 of CloverBootloader/a_bytes.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that i2d_ASN1_bytes passes to a, at line 131 of CloverBootloader/a_bytes.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	151	151

Object	a	a

Code Snippet
File Name CloverBootloader/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);
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=17
Status	New

The size of the buffer used by i2d_ASN1_OBJECT in a, at line 67 of CloverBootloader/a_object.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that i2d_ASN1_OBJECT passes to a, at line 67 of CloverBootloader/a_object.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/a_object.c	CloverBootloader/a_object.c
Line	79	79
Object	a	a

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

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

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=18
Status	New

The size of the buffer used by cms_EncryptedContent_init in keylen, at line 239 of CloverBootloader/cms_enc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cms_EncryptedContent_init passes to keylen, at line 239 of CloverBootloader/cms_enc.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/cms_enc.c	CloverBootloader/cms_enc.c
Line	249	249

Object	keylen	keylen

Code Snippet
File Name CloverBootloader/cms_enc.c
Method int cms_EncryptedContent_init(CMS_EncryptedContentInfo *ec,

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

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=19
Status	New

The size of the buffer used by EVP_MD_CTX_copy_ex in out, at line 291 of CloverBootloader/digest.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EVP_MD_CTX_copy_ex passes to out, at line 291 of CloverBootloader/digest.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/digest.c	CloverBootloader/digest.c
Line	330	330
Object	out	out

Code Snippet
File Name CloverBootloader/digest.c
Method int EVP_MD_CTX_copy_ex(EVP_MD_CTX *out, const EVP_MD_CTX *in)

```
....
330.              memcpy(out->md_data,in->md_data,out->digest-
>ctx_size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=20
Status	New

The size of the buffer used by aesni_gcm_init_key in gctx, at line 305 of CloverBootloader/e_aes.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that aesni_gcm_init_key passes to gctx, at line 305 of CloverBootloader/e_aes.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	335	335

Object	gctx	gctx

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aesni_gcm_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
335.                    memcpy(gctx->iv, iv, gctx->ivlen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=21
Status	New

The size of the buffer used by aes_gcm_ctrl in gctx, at line 700 of CloverBootloader/e_aes.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that aes_gcm_ctrl passes to gctx, at line 700 of CloverBootloader/e_aes.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	752	752
Object	gctx	gctx

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
752.                    memcpy(gctx->iv, ptr, gctx->ivlen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=22
Status	New

The size of the buffer used by aes_gcm_init_key in gctx, at line 817 of CloverBootloader/e_aes.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that aes_gcm_init_key passes to gctx, at line 817 of CloverBootloader/e_aes.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	873	873
Object	gctx	gctx

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
873.                    memcpy(gctx->iv, iv, gctx->ivlen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=23
Status	New

The size of the buffer used by aes_ccm_ctrl in arg, at line 1155 of CloverBootloader/e_aes.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that aes_ccm_ctrl passes to arg, at line 1155 of CloverBootloader/e_aes.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	1185	1185
Object	arg	arg

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_ccm_ctrl(EVP_CIPHER_CTX *c, int type, int arg, void *ptr)

```
....
1185.                   memcpy(c->buf, ptr, arg);
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=24
Status	New

The size of the buffer used by *ec_asn1_parameters2group in params, at line 747 of CloverBootloader/ec_asn1.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *ec_asn1_parameters2group passes to params, at line 747 of CloverBootloader/ec_asn1.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/ec_asn1.c	CloverBootloader/ec_asn1.c
Line	934	934
Object	params	params

Code Snippet

File Name	CloverBootloader/ec_asn1.c
Method	static EC_GROUP *ec_asn1_parameters2group(const ECPARAMETERS *params)

```
....
934.                        params->curve->seed->length);
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=25
Status	New

The size of the buffer used by ecdh_compute_key in outlen, at line 108 of CloverBootloader/ech_ossl.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ecdh_compute_key passes to outlen, at line 108 of CloverBootloader/ech_ossl.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/ech_ossl.c	CloverBootloader/ech_ossl.c
Line	205	205
Object	outlen	outlen

Code Snippet	
File Name	CloverBootloader/ech_ossl.c
Method	static int ecdh_compute_key(void *out, size_t outlen, const EC_POINT *pub_key,

```
....
205.                memcpy(out, buf, outlen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=26
Status	New

The size of the buffer used by EVP_CIPHER_CTX_copy in in, at line 647 of CloverBootloader/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_copy passes to in, at line 647 of CloverBootloader/evp_enc.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	674	674
Object	in	in

Code Snippet	
File Name	CloverBootloader/evp_enc.c

Method	int EVP_CIPHER_CTX_copy(EVP_CIPHER_CTX *out, const EVP_CIPHER_CTX *in)

```
....
674.              memcpy(out->cipher_data,in->cipher_data,in->cipher-
>ctx_size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=27
Status	New

The size of the buffer used by *CRYPTO_realloc_clean in old_len, at line 489 of CloverBootloader/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_realloc_clean passes to old_len, at line 489 of CloverBootloader/mem.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/mem.c	CloverBootloader/mem.c
Line	508	508
Object	old_len	old_len

Code Snippet	
File Name	CloverBootloader/mem.c
Method	void *CRYPTO_realloc_clean(void *str, int old_len, int num, const char *file,

```
....
508.              memcpy(ret,str,old_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=28
Status	New

The size of the buffer used by int_rsa_verify in sig, at line 154 of CloverBootloader/rsa_sign.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that int_rsa_verify passes to sig, at line 154 of CloverBootloader/rsa_sign.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/rsa_sign.c	CloverBootloader/rsa_sign.c
Line	283	283
Object	sig	sig

Code Snippet	
File Name	CloverBootloader/rsa_sign.c
Method	int int_rsa_verify(int dtype, const unsigned char *m,

```
....
283.                                                    sig->digest->length);
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=29
Status	New

The size of the buffer used by collect_data in plen, at line 1220 of CloverBootloader/tasn_dec.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that collect_data passes to plen, at line 1220 of CloverBootloader/tasn_dec.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/tasn_dec.c	CloverBootloader/tasn_dec.c
Line	1231	1231
Object	plen	plen

Code Snippet
File Name CloverBootloader/tasn_dec.c
Method static int collect_data(BUF_MEM *buf, const unsigned char **p, long plen)

```
....
1231.             memcpy(buf->data + len, *p, plen);
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=30
Status	New

The size of the buffer used by asn1_item_ex_combine_new in it, at line 88 of CloverBootloader/tasn_new.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that asn1_item_ex_combine_new passes to it, at line 88 of CloverBootloader/tasn_new.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/tasn_new.c	CloverBootloader/tasn_new.c
Line	166	166
Object	it	it

Code Snippet
File Name CloverBootloader/tasn_new.c
Method static int asn1_item_ex_combine_new(ASN1_VALUE **pval, const ASN1_ITEM *it,

```
....
166.                    memset(*pval, 0, it->size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=31
Status	New

The size of the buffer used by asn1_item_ex_combine_new in it, at line 88 of CloverBootloader/tasn_new.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that asn1_item_ex_combine_new passes to it, at line 88 of CloverBootloader/tasn_new.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/tasn_new.c	CloverBootloader/tasn_new.c
Line	194	194
Object	it	it

Code Snippet
File Name CloverBootloader/tasn_new.c
Method static int asn1_item_ex_combine_new(ASN1_VALUE **pval, const ASN1_ITEM *it,

```
....
194.                    memset(*pval, 0, it->size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=32
Status	New

The size of the buffer used by aes_ccm_cipher in cctx, at line 1239 of CloverBootloader/e_aes.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that aes_ccm_cipher passes to cctx, at line 1239 of CloverBootloader/e_aes.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	1293	1293
Object	cctx	cctx

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_ccm_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
1293.                           if (!memcmp(tag, ctx->buf, cctx->M))
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=33
Status	New

The size of the buffer used by obj_cmp in a, at line 385 of CloverBootloader/obj_dat.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that obj_cmp passes to a, at line 385 of CloverBootloader/obj_dat.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/obj_dat.c	CloverBootloader/obj_dat.c
Line	393	393
Object	a	a

Code Snippet
File Name CloverBootloader/obj_dat.c
Method static int obj_cmp(const ASN1_OBJECT * const *ap, const unsigned int *bp)

```
....
393.        return(memcmp(a->data,b->data,a->length));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=34
Status	New

The size of the buffer used by der_cmp in cmplen, at line 426 of CloverBootloader/tasn_enc.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that der_cmp passes to cmplen, at line 426 of CloverBootloader/tasn_enc.c, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	431	431
Object	cmplen	cmplen

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method static int der_cmp(const void *a, const void *b)

```
....
431.        i = memcmp(d1->data, d2->data, cmplen);
```

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=1020030&projectid=20025&pathid=252
Status	New

The variable declared in os at CloverBootloader/a_bytes.c in line 252 is not initialized when it is used by os at CloverBootloader/a_bytes.c in line 252.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	254	295
Object	os	os

Code Snippet
File Name CloverBootloader/a_bytes.c
Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

```
....
254.        ASN1_STRING *os=NULL;
....
295.              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=1020030&projectid=20025&pathid=253
Status	New

The variable declared in data at CloverBootloader/a_bytes.c in line 252 is not initialized when it is used by data at CloverBootloader/a_bytes.c in line 252.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c

Line	260	305
Object	data	data

Code Snippet
File Name CloverBootloader/a_bytes.c
Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

```
....
260.        b.data=NULL;
....
305.        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=1020030&projectid=20025&pathid=254
Status New

The variable declared in b at CloverBootloader/a_d2i_fp.c in line 87 is not initialized when it is used by data at CloverBootloader/a_d2i_fp.c in line 87.

	Source	Destination
File	CloverBootloader/a_d2i_fp.c	CloverBootloader/a_d2i_fp.c
Line	89	97
Object	b	data

Code Snippet
File Name CloverBootloader/a_d2i_fp.c
Method void *ASN1_d2i_bio(void *(*xnew)(void), d2i_of_void *d2i, BIO *in, void **x)

```
....
89.    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=1020030&projectid=20025&pathid=255
Status New

The variable declared in b at CloverBootloader/a_d2i_fp.c in line 106 is not initialized when it is used by data at CloverBootloader/a_d2i_fp.c in line 106.

	Source	Destination

File	CloverBootloader/a_d2i_fp.c	CloverBootloader/a_d2i_fp.c
Line	108	116
Object	b	data

Code Snippet
File Name CloverBootloader/a_d2i_fp.c
Method void *ASN1_item_d2i_bio(const ASN1_ITEM *it, BIO *in, void *x)

```
....
108.        BUF_MEM *b = NULL;
....
116.        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=1020030&projectid=20025&pathid=256
Status New

The variable declared in tkey at CloverBootloader/cms_enc.c in line 69 is not initialized when it is used by key at CloverBootloader/cms_enc.c in line 69.

	Source	Destination
File	CloverBootloader/cms_enc.c	CloverBootloader/cms_enc.c
Line	161	188
Object	tkey	key

Code Snippet
File Name CloverBootloader/cms_enc.c
Method BIO *cms_EncryptedContent_init_bio(CMS_EncryptedContentInfo *ec)

```
....
161.              tkey = NULL;
....
188.                              ec->key = tkey;
```

Use of Zero Initialized Pointer\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=257
Status New

The variable declared in tkey at CloverBootloader/cms_enc.c in line 69 is not initialized when it is used by key at CloverBootloader/cms_enc.c in line 69.

	Source	Destination
File	CloverBootloader/cms_enc.c	CloverBootloader/cms_enc.c
Line	76	188
Object	tkey	key

Code Snippet
File Name CloverBootloader/cms_enc.c
Method BIO *cms_EncryptedContent_init_bio(CMS_EncryptedContentInfo *ec)

```
....
76.   unsigned char *tkey = NULL;
....
188.                            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=1020030&projectid=20025&pathid=258
Status New

The variable declared in os1 at CloverBootloader/rsa_ameth.c in line 567 is not initialized when it is used by os2 at CloverBootloader/rsa_ameth.c in line 567.

	Source	Destination
File	CloverBootloader/rsa_ameth.c	CloverBootloader/rsa_ameth.c
Line	582	637
Object	os1	os2

Code Snippet
File Name CloverBootloader/rsa_ameth.c
Method static int rsa_item_sign(EVP_MD_CTX *ctx, const ASN1_ITEM *it, void *asn,

```
....
582.              ASN1_STRING *os1 = NULL, *os2 = NULL;
....
637.                    os2 = ASN1_STRING_dup(os1);
```

Use of Zero Initialized Pointer\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=259
Status New

The variable declared in p at CloverBootloader/tasn_dec.c in line 154 is not initialized when it is used by p at CloverBootloader/tasn_dec.c in line 154.

	Source	Destination
File	CloverBootloader/tasn_dec.c	CloverBootloader/tasn_dec.c
Line	163	294
Object	p	p

Code Snippet
File Name CloverBootloader/tasn_dec.c
Method int ASN1_item_ex_d2i(ASN1_VALUE **pval, const unsigned char **in, long len,

```
....
163.        const unsigned char *p = NULL, *q;
....
294.                    *wp = (unsigned char)((*p & V_ASN1_CONSTRUCTED)
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=260
Status New

The variable declared in wp at CloverBootloader/tasn_dec.c in line 154 is not initialized when it is used by wp at CloverBootloader/tasn_dec.c in line 154.

	Source	Destination
File	CloverBootloader/tasn_dec.c	CloverBootloader/tasn_dec.c
Line	164	301
Object	wp	wp

Code Snippet
File Name CloverBootloader/tasn_dec.c
Method int ASN1_item_ex_d2i(ASN1_VALUE **pval, const unsigned char **in, long len,

```
....
164.        unsigned char *wp=NULL; /* BIG FAT WARNING!  BREAKS CONST
WHERE USED */
....
301.                    *wp = imphack;
```

Use of Zero Initialized Pointer\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=261
Status New

The variable declared in p at CloverBootloader/tasn_enc.c in line 130 is not initialized when it is used by p at CloverBootloader/tasn_enc.c in line 130.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	134	193
Object	p	p

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int ASN1_item_ex_i2d(ASN1_VALUE **pval, unsigned char **out,

```
....
134.        unsigned char *p = NULL;
....
193.                    *p = aclass | tag | (*p & V_ASN1_CONSTRUCTED);
```

Use of Zero Initialized Pointer\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=262
Status New

The variable declared in p at CloverBootloader/tasn_enc.c in line 130 is not initialized when it is used by p at CloverBootloader/tasn_enc.c in line 130.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	134	193
Object	p	p

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int ASN1_item_ex_i2d(ASN1_VALUE **pval, unsigned char **out,

```
....
134.        unsigned char *p = NULL;
....
193.                    *p = aclass | tag | (*p & V_ASN1_CONSTRUCTED);
```

Use of Zero Initialized Pointer\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=263
Status New

The variable declared in s at CloverBootloader/a_bytes.c in line 66 is not initialized when it is used by ret at CloverBootloader/a_bytes.c in line 66.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	115	119
Object	s	ret

Code Snippet
File Name CloverBootloader/a_bytes.c
Method ASN1_STRING *d2i_ASN1_type_bytes(ASN1_STRING **a, const unsigned char **pp,

```
....
115.                s=NULL;
....
119.         ret->data=s;
```

Use of Zero Initialized Pointer\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=264
Status New

The variable declared in s at CloverBootloader/a_bytes.c in line 157 is not initialized when it is used by ret at CloverBootloader/a_bytes.c in line 157.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	228	233
Object	s	ret

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

```
....
228.                    s=NULL;
....
233.               ret->data=s;
```

Use of Zero Initialized Pointer\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=265
Status New

The variable declared in ln at CloverBootloader/a_object.c in line 286 is not initialized when it is used by ret at CloverBootloader/a_object.c in line 258.

	Source	Destination
File	CloverBootloader/a_object.c	CloverBootloader/a_object.c
Line	333	279
Object	ln	ret

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

```
....
333.        ret->ln=NULL;
```

File Name CloverBootloader/a_object.c

Method ASN1_OBJECT *d2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
279.        ret = c2i_ASN1_OBJECT(a, &p, len);
```

Use of Zero Initialized Pointer\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=266
Status New

The variable declared in sn at CloverBootloader/a_object.c in line 286 is not initialized when it is used by ret at CloverBootloader/a_object.c in line 258.

	Source	Destination
File	CloverBootloader/a_object.c	CloverBootloader/a_object.c
Line	332	279
Object	sn	ret

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

```
....
332.        ret->sn=NULL;
```

File Name CloverBootloader/a_object.c

Method	ASN1_OBJECT *d2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
279.        ret = c2i_ASN1_OBJECT(a, &p, len);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=267
Status	New

The variable declared in data at CloverBootloader/a_object.c in line 347 is not initialized when it is used by ret at CloverBootloader/a_object.c in line 258.

	Source	Destination
File	CloverBootloader/a_object.c	CloverBootloader/a_object.c
Line	358	279
Object	data	ret

Code Snippet

File Name	CloverBootloader/a_object.c
Method	ASN1_OBJECT *ASN1_OBJECT_new(void)

```
....
358.        ret->data=NULL;
```

File Name	CloverBootloader/a_object.c
Method	ASN1_OBJECT *d2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
279.        ret = c2i_ASN1_OBJECT(a, &p, len);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=268
Status	New

The variable declared in sn at CloverBootloader/a_object.c in line 347 is not initialized when it is used by ret at CloverBootloader/a_object.c in line 258.

	Source	Destination

File	CloverBootloader/a_object.c	CloverBootloader/a_object.c
Line	360	279
Object	sn	ret

Code Snippet
File Name CloverBootloader/a_object.c
Method ASN1_OBJECT *ASN1_OBJECT_new(void)

```
....
360.        ret->sn=NULL;
```

File Name CloverBootloader/a_object.c

Method ASN1_OBJECT *d2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
279.        ret = c2i_ASN1_OBJECT(a, &p, len);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=269
Status	New

The variable declared in ln at CloverBootloader/a_object.c in line 347 is not initialized when it is used by ret at CloverBootloader/a_object.c in line 258.

	Source	Destination
File	CloverBootloader/a_object.c	CloverBootloader/a_object.c
Line	361	279
Object	ln	ret

Code Snippet
File Name CloverBootloader/a_object.c
Method ASN1_OBJECT *ASN1_OBJECT_new(void)

```
....
361.        ret->ln=NULL;
```

File Name CloverBootloader/a_object.c

Method ASN1_OBJECT *d2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
279.        ret = c2i_ASN1_OBJECT(a, &p, len);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=270
Status	New

The variable declared in ln at CloverBootloader/a_object.c in line 347 is not initialized when it is used by data at CloverBootloader/a_object.c in line 286.

	Source	Destination
File	CloverBootloader/a_object.c	CloverBootloader/a_object.c
Line	361	316
Object	ln	data

Code Snippet

File Name CloverBootloader/a_object.c

Method ASN1_OBJECT *ASN1_OBJECT_new(void)

```
....
361.        ret->ln=NULL;
```

File Name CloverBootloader/a_object.c

Method ASN1_OBJECT *c2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
316.        data = (unsigned char *)ret->data;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=271
Status	New

The variable declared in sn at CloverBootloader/a_object.c in line 347 is not initialized when it is used by data at CloverBootloader/a_object.c in line 286.

	Source	Destination
File	CloverBootloader/a_object.c	CloverBootloader/a_object.c

Line	360	316
Object	sn	data

Code Snippet
File Name CloverBootloader/a_object.c
Method ASN1_OBJECT *ASN1_OBJECT_new(void)

```
....
360.        ret->sn=NULL;
```

File Name CloverBootloader/a_object.c

Method ASN1_OBJECT *c2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
316.        data = (unsigned char *)ret->data;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=272
Status	New

The variable declared in data at CloverBootloader/a_object.c in line 347 is not initialized when it is used by data at CloverBootloader/a_object.c in line 286.

	Source	Destination
File	CloverBootloader/a_object.c	CloverBootloader/a_object.c
Line	358	316
Object	data	data

Code Snippet
File Name CloverBootloader/a_object.c
Method ASN1_OBJECT *ASN1_OBJECT_new(void)

```
....
358.        ret->data=NULL;
```

File Name CloverBootloader/a_object.c

Method ASN1_OBJECT *c2i_ASN1_OBJECT(ASN1_OBJECT **a, const unsigned char **pp,

```
....
316.        data = (unsigned char *)ret->data;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=273
Status	New

The variable declared in os at CloverBootloader/pk7_lib.c in line 621 is not initialized when it is used by os at CloverBootloader/pk7_lib.c in line 621.

	Source	Destination
File	CloverBootloader/pk7_lib.c	CloverBootloader/pk7_lib.c
Line	654	661
Object	os	os

Code Snippet
File Name CloverBootloader/pk7_lib.c
Method int PKCS7_stream(unsigned char ***boundary, PKCS7 *p7)

```
....
654.              os = NULL;
....
661.        os->flags |= ASN1_STRING_FLAG_NDEF;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=274
Status	New

The variable declared in Pointer at CloverBootloader/rsa_ameth.c in line 268 is not initialized when it is used by mgf1md at CloverBootloader/rsa_ameth.c in line 460.

	Source	Destination
File	CloverBootloader/rsa_ameth.c	CloverBootloader/rsa_ameth.c
Line	275	497
Object	Pointer	mgf1md

Code Snippet
File Name CloverBootloader/rsa_ameth.c
Method static RSA_PSS_PARAMS *rsa_pss_decode(const X509_ALGOR *alg,

```
....
275.        *pmaskHash = NULL;
```

File Name CloverBootloader/rsa_ameth.c

Method static int rsa_item_verify(EVP_MD_CTX *ctx, const ASN1_ITEM *it, void *asn,

```
....
497.              mgf1md = EVP_get_digestbyobj(maskHash->algorithm);
```

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=1020030&projectid=20025&pathid=123
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 178 of CloverBootloader/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	CloverBootloader/a_int.c	CloverBootloader/a_int.c
Line	218	218
Object	AssignExpr	AssignExpr

Code Snippet

File Name CloverBootloader/a_int.c

Method ASN1_INTEGER *c2i_ASN1_INTEGER(ASN1_INTEGER **a, const unsigned char **pp,

```
....
218.              i = len;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=200

	25&pathid=124
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1239 of CloverBootloader/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	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	1294	1294
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_ccm_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
1294.                                   rv = len;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=125
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 886 of CloverBootloader/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	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	925	925
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_tls_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
925.              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=1020030&projectid=20025&pathid=126
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 886 of CloverBootloader/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	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	950	950
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_gcm_tls_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
950.                rv = len;
```

Integer Overflow\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=127
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 179 of CloverBootloader/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	CloverBootloader/e_aes_cbc_hmac_sha1.c	CloverBootloader/e_aes_cbc_hmac_sha1.c
Line	237	237
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
237.                    for (l=len-plen-1;plen<len;plen++) out[plen]=l;
```

Integer Overflow\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=128
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 179 of CloverBootloader/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	CloverBootloader/e_aes_cbc_hmac_sha1.c	CloverBootloader/e_aes_cbc_hmac_sha1.c
Line	280	280
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
280.                    maxpad = len-(SHA_DIGEST_LENGTH+1);
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=129
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 179 of CloverBootloader/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	CloverBootloader/e_aes_cbc_hmac_sha1.c	CloverBootloader/e_aes_cbc_hmac_sha1.c
Line	308	308
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
308.                    bitlen = key->md.Nl+(inp_len<<3);    /* at most
18 bits */
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=130

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 179 of CloverBootloader/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	CloverBootloader/e_aes_cbc_hmac_sha1.c	CloverBootloader/e_aes_cbc_hmac_sha1.c
Line	287	287
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
287.                    ret &= (int)mask;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=131
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 179 of CloverBootloader/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	CloverBootloader/e_aes_cbc_hmac_sha1.c	CloverBootloader/e_aes_cbc_hmac_sha1.c
Line	421	421
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
421.                            cmask = ((int)(j-off-
SHA_DIGEST_LENGTH))>>(sizeof(int)*8-1);
```

Integer Overflow\Path 10:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=132
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 179 of CloverBootloader/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	CloverBootloader/e_aes_cbc_hmac_sha1.c	CloverBootloader/e_aes_cbc_hmac_sha1.c
Line	423	423
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
423.                        cmask &= ((int)(off-1-j))>>(sizeof(int)*8-1);
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=133
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 116 of CloverBootloader/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	CloverBootloader/e_rc4_hmac_md5.c	CloverBootloader/e_rc4_hmac_md5.c
Line	188	188
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/e_rc4_hmac_md5.c
Method static int rc4_hmac_md5_cipher(EVP_CIPHER_CTX *ctx, unsigned char *out,

```
....
188.                    l = (key->md.Nl+(blocks<<3))&0xffffffffU;
```

Integer Overflow\Path 12:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=134
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 466 of CloverBootloader/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	CloverBootloader/obj_dat.c	CloverBootloader/obj_dat.c
Line	554	554
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/obj_dat.c
Method int OBJ_obj2txt(char *buf, int buf_len, const ASN1_OBJECT *a, int no_name)

```
....
554.                            i=(int)(l/40);
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=135
Status	New

A variable of a larger data type, hval, is being assigned to a smaller data type, in 25345 of CloverBootloader/unicode_property_data.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	CloverBootloader/unicode_property_data.c	CloverBootloader/unicode_property_data.c
Line	25376	25376
Object	hval	hval

Code Snippet
File Name CloverBootloader/unicode_property_data.c
Method hash (register const char *str, register size_t len)

```
....
25376.    register unsigned int hval = (unsigned int )len;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=136

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 169 of CloverBootloader/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	CloverBootloader/b_print.c	CloverBootloader/b_print.c
Line	190	190
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/b_print.c
Method _dopr(

```
....
190.      flags = currlen = cflags = min = 0;
```

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=1020030&projectid=20025&pathid=239
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by flags at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	672
Object	strtmp	flags

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
672.                    && (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=1020030&projectid=20025&pathid=240
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by type at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	591
Object	strtmp	type

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
591.              utype = strtmp->type;
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=241
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by data at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	676
Object	strtmp	data

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
676.                            strtmp->data = cout;
```

Use of Uninitialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=242
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by length at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	677
Object	strtmp	length

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
677.                            strtmp->length = 0;
```

Use of Uninitialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=243
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by data at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	682
Object	strtmp	data

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
682.              cont = strtmp->data;
```

Use of Uninitialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=244
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by length at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	683
Object	strtmp	length

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
683.              len = strtmp->length;
```

Use of Uninitialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=245
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by flags at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	672
Object	strtmp	flags

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
672.                    && (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=1020030&projectid=20025&pathid=246
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by data at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	676
Object	strtmp	data

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
676.                            strtmp->data = cout;
```

Use of Uninitialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=247
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by length at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	677
Object	strtmp	length

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
677.                            strtmp->length = 0;
```

Use of Uninitialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=248
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by data at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	682
Object	strtmp	data

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
682.              cont = strtmp->data;
```

Use of Uninitialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=249
Status	New

The variable declared in strtmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by length at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	569	683
Object	strtmp	length

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
569.        ASN1_STRING *strtmp;
....
683.              len = strtmp->length;
```

Use of Uninitialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=250
Status	New

The variable declared in otmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by otmp at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	570	610
Object	otmp	otmp

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
570.        ASN1_OBJECT *otmp;
....
610.              len = otmp->length;
```

Use of Uninitialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=251
Status	New

The variable declared in otmp at CloverBootloader/tasn_enc.c in line 565 is not initialized when it is used by data at CloverBootloader/tasn_enc.c in line 565.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	570	609
Object	otmp	data

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method int asn1_ex_i2c(ASN1_VALUE **pval, unsigned char *cout, int *putype,

```
....
570.        ASN1_OBJECT *otmp;
....
609.              cont = otmp->data;
```

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=1020030&projectid=20025&pathid=35
Status	New

The function size in CloverBootloader/regcomp.c at line 114 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	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	121	121
Object	size	size

Code Snippet
File Name CloverBootloader/regcomp.c
Method ops_init(regex_t* reg, int init_alloc_size)

```
....
121.      p = (Operation* )xmalloc(size);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=36
Status	New

The function size in CloverBootloader/regcomp.c at line 114 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	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	127	127
Object	size	size

Code Snippet
File Name CloverBootloader/regcomp.c
Method ops_init(regex_t* reg, int init_alloc_size)

```
....
127.        cp = (enum OpCode* )xmalloc(size);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=37
Status	New

The function len in CloverBootloader/regcomp.c at line 834 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	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	840	840
Object	len	len

Code Snippet
File Name CloverBootloader/regcomp.c
Method set_multi_byte_cclass(BBuf* mbuf, regex_t* reg)

```
....
840.    p = xmalloc(len);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=38
Status	New

The function size in CloverBootloader/regcomp.c at line 149 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	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	164	164
Object	size	size

Code Snippet
File Name CloverBootloader/regcomp.c
Method ops_expand(regex_t* reg, int n)

```
....
164.    p = (Operation* )xrealloc(reg->ops, size, sizeof(Operation) *
reg->ops_alloc);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=39
Status	New

The function size in CloverBootloader/regcomp.c at line 149 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	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	169	169
Object	size	size

Code Snippet
File Name CloverBootloader/regcomp.c
Method ops_expand(regex_t* reg, int n)

```
....
169.    cp = (enum OpCode* )xrealloc(reg->ocs, size, sizeof(enum OpCode)
* reg->ops_alloc);
```

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=1020030&projectid=20025&pathid=137
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 590 of CloverBootloader/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	CloverBootloader/b_print.c	CloverBootloader/b_print.c
Line	593	593
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/b_print.c
Method roundv(LDOUBLE value)

```
....
593.      intpart = (long) value;
```

Long Overflow\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=138
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 601 of CloverBootloader/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	CloverBootloader/b_print.c	CloverBootloader/b_print.c
Line	634	634
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/b_print.c
Method fmtfp(

```
....
634.      intpart = (long)ufvalue;
```

Heap Inspection

Query Path:
CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

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=1020030&projectid=20025&pathid=236
Status	New

Method SRP_VBASE_init at line 360 of CloverBootloader/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	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	369	369
Object	user_pwd	user_pwd

Code Snippet
File Name CloverBootloader/srp_vfy.c
Method int SRP_VBASE_init(SRP_VBASE *vb, char *verifier_file)

```
....
369.        SRP_user_pwd *user_pwd = NULL ;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=237
Status	New

Method CMS_RecipientInfo_set0_password at line 65 of CloverBootloader/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	CloverBootloader/cms_pwri.c	CloverBootloader/cms_pwri.c
Line	66	66
Object	passlen	passlen

Code Snippet
File Name CloverBootloader/cms_pwri.c
Method int CMS_RecipientInfo_set0_password(CMS_RecipientInfo *ri,

```
....
66.                         unsigned char *pass, ossl_ssize_t passlen)
```

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=1020030&projectid=20025&pathid=7
Status	New

The application performs an illegal operation in distance_multiply, in CloverBootloader/regcomp.c. In line 467, the program attempts to divide by m, 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 m in distance_multiply of CloverBootloader/regcomp.c, at line 467.

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	471	471
Object	m	m

Code Snippet
File Name CloverBootloader/regcomp.c
Method distance_multiply(OnigLen d, int m)

```
....
471.    if (d < INFINITE_LEN / m)
```

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=1020030&projectid=20025&pathid=11
Status	New

The pointer d2 at CloverBootloader/tasn_enc.c in line 426 is being used after it has been freed.

	Source	Destination
File	CloverBootloader/tasn_enc.c	CloverBootloader/tasn_enc.c
Line	434	434
Object	d2	d2

Code Snippet
File Name CloverBootloader/tasn_enc.c
Method static int der_cmp(const void *a, const void *b)

```
....
434.        return d1->length - d2->length;
```

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=1020030&projectid=20025&pathid=122
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 335 of CloverBootloader/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	CloverBootloader/a_int.c	CloverBootloader/a_int.c
Line	365	365
Object	AssignExpr	AssignExpr

Code Snippet
File Name CloverBootloader/a_int.c
Method int ASN1_INTEGER_set(ASN1_INTEGER *a, long v)

```
....
365.            buf[i]=(int)d&0xff;
```

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=1020030&projectid=20025&pathid=238
Status	New

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	136	136
Object	buf	buf

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
136.    char* buf = (char*)malloc(st.st_size+1);
```

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=1020030&projectid=20025&pathid=398
Status	New

The application protects passwords with SHA1_Final in aesni_cbc_hmac_sha1_ctrl, of CloverBootloader/e_aes_cbc_hmac_sha1.c at line 456, 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	CloverBootloader/e_aes_cbc_hmac_sha1.c	CloverBootloader/e_aes_cbc_hmac_sha1.c
Line	470	472
Object	Address	SHA1_Final

Code Snippet
File Name CloverBootloader/e_aes_cbc_hmac_sha1.c
Method static int aesni_cbc_hmac_sha1_ctrl(EVP_CIPHER_CTX *ctx, int type, int arg, void *ptr)

```
....
470.                    SHA1_Init(&key->head);
....
472.                    SHA1_Final(hmac_key,&key->head);
```

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=1020030&projectid=20025&pathid=275
Status	New

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	33	33
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name CloverBootloader/main.cpp
Method ssize_t read_all(int fd, void* buf, size_t size)

```
....
33.      ssize_t nblu = read(fd, ((uint8_t*)buf)+nbluTotal, MIN(65536,
size-nbluTotal));
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=276
Status	New

	Source	Destination
File	CloverBootloader/EfiUtilityMsgs.c	CloverBootloader/EfiUtilityMsgs.c
Line	449	449
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/EfiUtilityMsgs.c
Method PrintMessage (

```
....
449.        fprintf (stdout, "%04d-%02d-%02d %02d:%02d:%02d",
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=277
Status	New

	Source	Destination
File	CloverBootloader/EfiUtilityMsgs.c	CloverBootloader/EfiUtilityMsgs.c
Line	472	472
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/EfiUtilityMsgs.c
Method PrintMessage (

```
....
472.          fprintf (stdout, "%s...\n", mUtilityName);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=278
Status	New

	Source	Destination
File	CloverBootloader/EfiUtilityMsgs.c	CloverBootloader/EfiUtilityMsgs.c
Line	507	507
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/EfiUtilityMsgs.c
Method PrintMessage (

```
....
507.    fprintf (stdout, "%s", Line);
```

Improper Resource Access Authorization\Path 5:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=279
Status	New

	Source	Destination
File	CloverBootloader/EfiUtilityMsgs.c	CloverBootloader/EfiUtilityMsgs.c
Line	512	512
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/EfiUtilityMsgs.c
Method PrintMessage (

```
....
512.      fprintf (stdout, ": %s", Text);
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=280
Status	New

	Source	Destination
File	CloverBootloader/EfiUtilityMsgs.c	CloverBootloader/EfiUtilityMsgs.c
Line	514	514
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/EfiUtilityMsgs.c
Method PrintMessage (

```
....
514.    fprintf (stdout, "\n");
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=281
Status	New

	Source	Destination
File	CloverBootloader/EfiUtilityMsgs.c	CloverBootloader/EfiUtilityMsgs.c
Line	521	521

Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/EfiUtilityMsgs.c
Method PrintMessage (

```
....
521.      fprintf (stdout, "  %s\n", Line2);
```

Improper Resource Access Authorization\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=282
Status New

	Source	Destination
File	CloverBootloader/EfiUtilityMsgs.c	CloverBootloader/EfiUtilityMsgs.c
Line	551	551
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/EfiUtilityMsgs.c
Method PrintSimpleMessage (

```
....
551.      fprintf (stdout, "%s\n", Line);
```

Improper Resource Access Authorization\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=283
Status New

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	98	98
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
98.          fprintf(stderr, "ConfigPlistValidator for '%s'\n",
gRevisionStr);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=284
Status	New

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	99	99
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
99.          fprintf(stderr, "Build id is '%s'\n", gBuildId.c_str());
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=285
Status	New

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	107	107
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
107.          fprintf(stderr, "Bug in argument parsing.\n");
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=286
Status	New

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	132	132
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
132.      fprintf(stderr, "Cannot stat file '%s'\n", path);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=287
Status	New

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	140	140
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
140.      fprintf(stderr, "Cannot open file '%s'. Errno %s\n", path,
strerror(errno));
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=288
Status	New

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp

Line	145	145
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
145.      fprintf(stderr, "Cannot read file '%s'. Errno %s\n", path,
strerror(errno));
```

Improper Resource Access Authorization\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=289
Status New

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	51	51
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/main.cpp
Method void usage()

```
....
51.    fprintf(stderr, "Usage ConfigPlistValidator [-h|--help] [-v|--
version] [--info]  [-p|--productname=] path_to_config.plist\n");
```

Improper Resource Access Authorization\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=290
Status New

	Source	Destination
File	CloverBootloader/mem.c	CloverBootloader/mem.c
Line	399	399
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/mem.c
Method void *CRYPTO_malloc_locked(int num, const char *file, int line)

```
....
399.        fprintf(stderr, "LEVITTE_DEBUG_MEM:          > 0x%p (%d)\n",
ret, num);
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=291
Status	New

	Source	Destination
File	CloverBootloader/mem.c	CloverBootloader/mem.c
Line	422	422
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/mem.c
Method void CRYPTO_free_locked(void *str)

```
....
422.        fprintf(stderr, "LEVITTE_DEBUG_MEM:          < 0x%p\n", str);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=292
Status	New

	Source	Destination
File	CloverBootloader/mem.c	CloverBootloader/mem.c
Line	443	443
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/mem.c
Method void *CRYPTO_malloc(int num, const char *file, int line)

```
....
443.        fprintf(stderr, "LEVITTE_DEBUG_MEM:          > 0x%p (%d)\n",
ret, num);
```

Improper Resource Access Authorization\Path 19:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=293
Status	New

	Source	Destination
File	CloverBootloader/mem.c	CloverBootloader/mem.c
Line	481	481
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/mem.c
Method void *CRYPTO_realloc(void *str, int num, const char *file, int line)

```
....
481.         fprintf(stderr, "LEVITTE_DEBUG_MEM:          | 0x%p -> 0x%p
(%d)\n", str, ret, num);
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=294
Status	New

	Source	Destination
File	CloverBootloader/mem.c	CloverBootloader/mem.c
Line	513	513
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/mem.c
Method void *CRYPTO_realloc_clean(void *str, int old_len, int num, const char *file,

```
....
513.         fprintf(stderr,
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=295
Status	New

	Source	Destination

File	CloverBootloader/mem.c	CloverBootloader/mem.c
Line	528	528
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/mem.c
Method void CRYPTO_free(void *str)

```
....
528.        fprintf(stderr, "LEVITTE_DEBUG_MEM:          < 0x%p\n", str);
```

Improper Resource Access Authorization\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=296
Status New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	2068	2068
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method compile_tree(Node* node, regex_t* reg, ScanEnv* env)

```
....
2068.      fprintf(stderr, "compile_tree: undefined node type %d\n",
NODE_TYPE(node));
```

Improper Resource Access Authorization\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=297
Status New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	5887	5887
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c

Method	optimize_nodes(Node* node, OptNode* opt, OptEnv* env)

```
....
5887.      fprintf(stderr, "optimize_nodes: undefined node type %d\n",
NODE_TYPE(node));
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=298
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6059	6059
Object	fprintf	fprintf

Code Snippet	
File Name	CloverBootloader/regcomp.c
Method	static void print_enc_string(FILE* fp, OnigEncoding enc,

```
....
6059.    fprintf(fp, "\nPATTERN: /");
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=299
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6069	6069
Object	fprintf	fprintf

Code Snippet	
File Name	CloverBootloader/regcomp.c
Method	static void print_enc_string(FILE* fp, OnigEncoding enc,

```
....
6069.          fprintf(fp, " 0x%04x ", (int )code);
```

Improper Resource Access Authorization\Path 26:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=300
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6085	6085
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method static void print_enc_string(FILE* fp, OnigEncoding enc,

```
....
6085.    fprintf(fp, "/\n");
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=301
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6098	6098
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_distance_range(FILE* f, OnigLen a, OnigLen b)

```
....
6098.      fprintf(f, "(%u)", a);
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=302
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c

Line	6105	6105
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_distance_range(FILE* f, OnigLen a, OnigLen b)

```
....
6105.       fprintf(f, "(%u)", b);
```

Improper Resource Access Authorization\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=303
Status New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6113	6113
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6113.     fprintf(f, "[");
```

Improper Resource Access Authorization\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=304
Status New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6116	6116
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6116.       fprintf(f, "begin-buf");
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=305
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6120	6120
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6120.       if (q) fprintf(f, ", ");
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=306
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6122	6122
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6122.       fprintf(f, "begin-line");
```

Improper Resource Access Authorization\Path 33:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=307
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6125	6125
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6125.       if (q) fprintf(f, ", ");
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=308
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6127	6127
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6127.       fprintf(f, "begin-pos");
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=309
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6130	6130

Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6130.       if (q) fprintf(f, ", ");
```

Improper Resource Access Authorization\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=310
Status New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6132	6132
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6132.       fprintf(f, "end-buf");
```

Improper Resource Access Authorization\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=311
Status New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6135	6135
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6135.       if (q) fprintf(f, ", ");
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=312
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6137	6137
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6137.       fprintf(f, "semi-end-buf");
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=313
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6140	6140
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6140.       if (q) fprintf(f, ", ");
```

Improper Resource Access Authorization\Path 40:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=314
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6142	6142
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6142.       fprintf(f, "end-line");
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=315
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6145	6145
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6145.       if (q) fprintf(f, ", ");
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=316
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6147	6147

Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6147.       fprintf(f, "anychar-inf");
```

Improper Resource Access Authorization\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=317
Status New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6150	6150
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6150.       if (q) fprintf(f, ", ");
```

Improper Resource Access Authorization\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=318
Status New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6151	6151
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6151.       fprintf(f, "anychar-inf-ml");
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=319
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6154	6154
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_anchor(FILE* f, int anchor)

```
....
6154.     fprintf(f, "]");
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=320
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6164	6164
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_optimize_info(FILE* f, regex_t* reg)

```
....
6164.     fprintf(f, "optimize: %s\n", on[reg->optimize]);
```

Improper Resource Access Authorization\Path 47:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=321
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6165	6165
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_optimize_info(FILE* f, regex_t* reg)

```
....
6165.    fprintf(f, "  anchor: "); print_anchor(f, reg->anchor);
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=322
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6168	6168
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_optimize_info(FILE* f, regex_t* reg)

```
....
6168.    fprintf(f, "\n");
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=323
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6171	6171

Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_optimize_info(FILE* f, regex_t* reg)

```
....
6171.       fprintf(f, "  sub anchor: "); print_anchor(f, reg-
>sub_anchor);
```

Improper Resource Access Authorization\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=324
Status New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6172	6172
Object	fprintf	fprintf

Code Snippet
File Name CloverBootloader/regcomp.c
Method print_optimize_info(FILE* f, regex_t* reg)

```
....
6172.       fprintf(f, "\n");
```

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=1020030&projectid=20025&pathid=40
Status New

The variable declared in null at CloverBootloader/a_bytes.c in line 252 is not initialized when it is used by data at CloverBootloader/a_bytes.c in line 252.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	254	295
Object	null	data

Code Snippet
File Name CloverBootloader/a_bytes.c
Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

```
....
254.        ASN1_STRING *os=NULL;
....
295.              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=1020030&projectid=20025&pathid=41
Status New

The variable declared in null at CloverBootloader/e_aes.c in line 229 is not initialized when it is used by cbc at CloverBootloader/e_aes.c in line 229.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	243	241
Object	null	cbc

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aesni_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
243.                                  NULL;
....
241.              dat->stream.cbc    = mode==EVP_CIPH_CBC_MODE ?
```

NULL Pointer Dereference\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=42
Status New

The variable declared in null at CloverBootloader/e_aes.c in line 496 is not initialized when it is used by cbc at CloverBootloader/e_aes.c in line 496.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	521	519
Object	null	cbc

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
521.                                    NULL;
....
519.                dat->stream.cbc     = mode==EVP_CIPH_CBC_MODE ?
```

NULL Pointer Dereference\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=43
Status New

The variable declared in null at CloverBootloader/e_aes.c in line 496 is not initialized when it is used by cbc at CloverBootloader/e_aes.c in line 496.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	530	528
Object	null	cbc

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
530.                                    NULL;
....
528.                dat->stream.cbc     = mode==EVP_CIPH_CBC_MODE ?
```

NULL Pointer Dereference\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=44
Status New

The variable declared in null at CloverBootloader/e_aes.c in line 496 is not initialized when it is used by cbc at CloverBootloader/e_aes.c in line 496.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	549	547
Object	null	cbc

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
549.                                    NULL;
....
547.                dat->stream.cbc     = mode==EVP_CIPH_CBC_MODE ?
```

NULL Pointer Dereference\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=45
Status New

The variable declared in null at CloverBootloader/e_aes.c in line 496 is not initialized when it is used by cbc at CloverBootloader/e_aes.c in line 496.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	558	556
Object	null	cbc

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_init_key(EVP_CIPHER_CTX *ctx, const unsigned char *key,

```
....
558.                                    NULL;
....
556.                dat->stream.cbc     = mode==EVP_CIPH_CBC_MODE ?
```

NULL Pointer Dereference\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=46
Status New

The variable declared in null at CloverBootloader/pk7_lib.c in line 621 is not initialized when it is used by flags at CloverBootloader/pk7_lib.c in line 621.

	Source	Destination
File	CloverBootloader/pk7_lib.c	CloverBootloader/pk7_lib.c
Line	654	661
Object	null	flags

Code Snippet
File Name CloverBootloader/pk7_lib.c
Method int PKCS7_stream(unsigned char ***boundary, PKCS7 *p7)

```
....
654.                os = NULL;
....
661.        os->flags |= ASN1_STRING_FLAG_NDEF;
```

NULL Pointer Dereference\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=47
Status New

The variable declared in null at CloverBootloader/regcomp.c in line 6038 is not initialized when it is used by exact_end at CloverBootloader/regcomp.c in line 6038.

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	6045	6045
Object	null	exact_end

Code Snippet
File Name CloverBootloader/regcomp.c
Method clear_optimize_info(regex_t* reg)

```
....
6045.    reg->exact_end     = (UChar* )NULL;
```

NULL Pointer Dereference\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=48
Status New

The variable declared in null at CloverBootloader/srp_vfy.c in line 360 is not initialized when it is used by info at CloverBootloader/srp_vfy.c in line 182.

	Source	Destination

File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	434	189
Object	null	info

Code Snippet
File Name CloverBootloader/srp_vfy.c
Method int SRP_VBASE_init(SRP_VBASE *vb, char *verifier_file)

```
....
434.                        user_pwd = NULL; /* abandon responsability
*/
```

File Name CloverBootloader/srp_vfy.c

Method static void SRP_user_pwd_free(SRP_user_pwd *user_pwd)

```
....
189.        OPENSSL_free(user_pwd->info);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=49
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 360 is not initialized when it is used by info at CloverBootloader/srp_vfy.c in line 182.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	369	189
Object	null	info

Code Snippet
File Name CloverBootloader/srp_vfy.c
Method int SRP_VBASE_init(SRP_VBASE *vb, char *verifier_file)

```
....
369.        SRP_user_pwd *user_pwd = NULL ;
```

File Name CloverBootloader/srp_vfy.c

Method static void SRP_user_pwd_free(SRP_user_pwd *user_pwd)

```
....
189.        OPENSSL_free(user_pwd->info);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=50
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 360 is not initialized when it is used by id at CloverBootloader/srp_vfy.c in line 182.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	434	188
Object	null	id

Code Snippet

File Name CloverBootloader/srp_vfy.c

Method int SRP_VBASE_init(SRP_VBASE *vb, char *verifier_file)

```
....
434.                        user_pwd = NULL; /* abandon responsability
*/
```

File Name CloverBootloader/srp_vfy.c

Method static void SRP_user_pwd_free(SRP_user_pwd *user_pwd)

```
....
188.        OPENSSL_free(user_pwd->id);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=51
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 360 is not initialized when it is used by id at CloverBootloader/srp_vfy.c in line 182.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	369	188

Object	null	id

Code Snippet
File Name CloverBootloader/srp_vfy.c
Method int SRP_VBASE_init(SRP_VBASE *vb, char *verifier_file)

```
....
369.        SRP_user_pwd *user_pwd = NULL ;
```

File Name CloverBootloader/srp_vfy.c
Method static void SRP_user_pwd_free(SRP_user_pwd *user_pwd)

```
....
188.        OPENSSL_free(user_pwd->id);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=52
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 360 is not initialized when it is used by v at CloverBootloader/srp_vfy.c in line 182.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	434	187
Object	null	v

Code Snippet
File Name CloverBootloader/srp_vfy.c
Method int SRP_VBASE_init(SRP_VBASE *vb, char *verifier_file)

```
....
434.                        user_pwd = NULL; /* abandon responsability
*/
```

File Name CloverBootloader/srp_vfy.c
Method static void SRP_user_pwd_free(SRP_user_pwd *user_pwd)

```
....
187.        BN_clear_free(user_pwd->v);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=53
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 360 is not initialized when it is used by v at CloverBootloader/srp_vfy.c in line 182.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	369	187
Object	null	v

Code Snippet
File Name CloverBootloader/srp_vfy.c
Method int SRP_VBASE_init(SRP_VBASE *vb, char *verifier_file)

```
....
369.        SRP_user_pwd *user_pwd = NULL ;
```

File Name CloverBootloader/srp_vfy.c
Method static void SRP_user_pwd_free(SRP_user_pwd *user_pwd)

```
....
187.        BN_clear_free(user_pwd->v);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=54
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 475 is not initialized when it is used by v at CloverBootloader/srp_vfy.c in line 182.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	513	187
Object	null	v

Code Snippet
File Name CloverBootloader/srp_vfy.c
Method SRP_user_pwd *SRP_VBASE_get_by_user(SRP_VBASE *vb, char *username)

```
....
513.        if (SRP_user_pwd_set_sv_BN(user,
BN_bin2bn(digs,SHA_DIGEST_LENGTH,NULL),
BN_bin2bn(digv,SHA_DIGEST_LENGTH, NULL)))
```

File Name CloverBootloader/srp_vfy.c

Method static void SRP_user_pwd_free(SRP_user_pwd *user_pwd)

```
....
187.        BN_clear_free(user_pwd->v);
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=55
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 360 is not initialized when it is used by s at CloverBootloader/srp_vfy.c in line 182.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	434	186
Object	null	s

Code Snippet

File Name CloverBootloader/srp_vfy.c

Method int SRP_VBASE_init(SRP_VBASE *vb, char *verifier_file)

```
....
434.                        user_pwd = NULL; /* abandon responsability
*/
```

File Name CloverBootloader/srp_vfy.c

Method static void SRP_user_pwd_free(SRP_user_pwd *user_pwd)

```
....
186.        BN_free(user_pwd->s);
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=200

	25&pathid=56
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 360 is not initialized when it is used by s at CloverBootloader/srp_vfy.c in line 182.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	369	186
Object	null	s

Code Snippet
File Name CloverBootloader/srp_vfy.c
Method int SRP_VBASE_init(SRP_VBASE *vb, char *verifier_file)

```
....
369.        SRP_user_pwd *user_pwd = NULL ;
```

File Name CloverBootloader/srp_vfy.c
Method static void SRP_user_pwd_free(SRP_user_pwd *user_pwd)

```
....
186.        BN_free(user_pwd->s);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=57
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 475 is not initialized when it is used by s at CloverBootloader/srp_vfy.c in line 182.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	513	186
Object	null	s

Code Snippet
File Name CloverBootloader/srp_vfy.c
Method SRP_user_pwd *SRP_VBASE_get_by_user(SRP_VBASE *vb, char *username)

```
....
513.        if (SRP_user_pwd_set_sv_BN(user,
BN_bin2bn(digs,SHA_DIGEST_LENGTH,NULL),
BN_bin2bn(digv,SHA_DIGEST_LENGTH, NULL)))
```

File Name CloverBootloader/srp_vfy.c

Method static void SRP_user_pwd_free(SRP_user_pwd *user_pwd)

```
....
186.        BN_free(user_pwd->s);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=58
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 475 is not initialized when it is used by s at CloverBootloader/srp_vfy.c in line 237.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	513	241
Object	null	s

Code Snippet

File Name CloverBootloader/srp_vfy.c

Method SRP_user_pwd *SRP_VBASE_get_by_user(SRP_VBASE *vb, char *username)

```
....
513.        if (SRP_user_pwd_set_sv_BN(user,
BN_bin2bn(digs,SHA_DIGEST_LENGTH,NULL),
BN_bin2bn(digv,SHA_DIGEST_LENGTH, NULL)))
```

File Name CloverBootloader/srp_vfy.c

Method static int SRP_user_pwd_set_sv_BN(SRP_user_pwd *vinfo, BIGNUM *s, BIGNUM *v)

```
....
241.        return (vinfo->s != NULL && vinfo->v != NULL) ;
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=59
Status	New

The variable declared in null at CloverBootloader/srp_vfy.c in line 475 is not initialized when it is used by v at CloverBootloader/srp_vfy.c in line 237.

	Source	Destination
File	CloverBootloader/srp_vfy.c	CloverBootloader/srp_vfy.c
Line	513	241
Object	null	v

Code Snippet
File Name CloverBootloader/srp_vfy.c
Method SRP_user_pwd *SRP_VBASE_get_by_user(SRP_VBASE *vb, char *username)

```
....
513.        if (SRP_user_pwd_set_sv_BN(user,
BN_bin2bn(digs,SHA_DIGEST_LENGTH,NULL),
BN_bin2bn(digv,SHA_DIGEST_LENGTH, NULL)))
```

File Name CloverBootloader/srp_vfy.c
Method static int SRP_user_pwd_set_sv_BN(SRP_user_pwd *vinfo, BIGNUM *s, BIGNUM *v)

```
....
241.        return (vinfo->s != NULL && vinfo->v != NULL) ;
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=60
Status	New

The variable declared in 0 at CloverBootloader/a_bytes.c in line 157 is not initialized when it is used by max at CloverBootloader/a_bytes.c in line 157.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	198	198
Object	0	max

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

```
....
198.              c.max=(length == 0)?0:(p+length);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=61
Status	New

The variable declared in 0 at CloverBootloader/a_bytes.c in line 157 is not initialized when it is used by p at CloverBootloader/a_bytes.c in line 252.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	198	283
Object	0	p

Code Snippet

File Name CloverBootloader/a_bytes.c

Method ASN1_STRING *d2i_ASN1_bytes(ASN1_STRING **a, const unsigned char **pp,

```
....
198.              c.max=(length == 0)?0:(p+length);
```

File Name CloverBootloader/a_bytes.c

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

```
....
283.              if (d2i_ASN1_bytes(&os,&c->p,c->max-c->p,c->tag,c-
>xclass)
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=62
Status	New

The variable declared in 0 at CloverBootloader/a_bytes.c in line 157 is not initialized when it is used by p at CloverBootloader/a_bytes.c in line 252.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	198	283

Object	0	p

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

```
....
198.            c.max=(length == 0)?0:(p+length);
```

File Name CloverBootloader/a_bytes.c

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

```
....
283.            if (d2i_ASN1_bytes(&os,&c->p,c->max-c->p,c->tag,c-
>xclass)
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=63
Status	New

The variable declared in 0 at CloverBootloader/a_bytes.c in line 157 is not initialized when it is used by tag at CloverBootloader/a_bytes.c in line 252.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	198	283
Object	0	tag

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

```
....
198.            c.max=(length == 0)?0:(p+length);
```

File Name CloverBootloader/a_bytes.c

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

```
....
283.            if (d2i_ASN1_bytes(&os,&c->p,c->max-c->p,c->tag,c-
>xclass)
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=64
Status	New

The variable declared in 0 at CloverBootloader/a_bytes.c in line 157 is not initialized when it is used by xclass at CloverBootloader/a_bytes.c in line 252.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	198	283
Object	0	xclass

Code Snippet

File Name CloverBootloader/a_bytes.c

Method ASN1_STRING *d2i_ASN1_bytes(ASN1_STRING **a, const unsigned char **pp,

```
....
198.              c.max=(length == 0)?0:(p+length);
```

File Name CloverBootloader/a_bytes.c

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

```
....
283.              if (d2i_ASN1_bytes(&os,&c->p,c->max-c->p,c->tag,c-
>xclass)
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=65
Status	New

The variable declared in 0 at CloverBootloader/a_bytes.c in line 157 is not initialized when it is used by max at CloverBootloader/a_bytes.c in line 252.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	198	283
Object	0	max

Code Snippet

File Name CloverBootloader/a_bytes.c

Method	ASN1_STRING *d2i_ASN1_bytes(ASN1_STRING **a, const unsigned char **pp,

```
....
198.                c.max=(length == 0)?0:(p+length);
```

File Name	CloverBootloader/a_bytes.c
Method	static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

```
....
283.                if (d2i_ASN1_bytes(&os,&c->p,c->max-c->p,c->tag,c-
>xclass)
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=66
Status	New

The variable declared in 0 at CloverBootloader/regcomp.c in line 114 is not initialized when it is used by ocs at CloverBootloader/regcomp.c in line 114.

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	136	136
Object	0	ocs

Code Snippet	
File Name	CloverBootloader/regcomp.c
Method	ops_init(regex_t* reg, int init_alloc_size)

```
....
136.      reg->ocs = (enum OpCode* )0;
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=67
Status	New

The variable declared in 0 at CloverBootloader/regcomp.c in line 1586 is not initialized when it is used by not at CloverBootloader/regcomp.c in line 1586.

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c

Line	1635	1634
Object	0	not

Code Snippet
File Name CloverBootloader/regcomp.c
Method compile_anchor_node(AnchorNode* node, regex_t* reg, ScanEnv* env)

```
....
1635.           (node->type == ANCR_NO_TEXT_SEGMENT_BOUNDARY ? 1 : 0);
....
1634.         COP(reg)->text_segment_boundary.not =
```

NULL Pointer Dereference\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=68
Status New

The variable declared in 0 at CloverBootloader/regcomp.c in line 2354 is not initialized when it is used by char_len at CloverBootloader/regcomp.c in line 2354.

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	2360	2453
Object	0	char_len

Code Snippet
File Name CloverBootloader/regcomp.c
Method get_char_len_node1(Node* node, regex_t* reg, int* len, int level)

```
....
2360.    *len = 0;
....
2453.               en->char_len = *len;
```

NULL Pointer Dereference\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=69
Status New

The variable declared in 0 at CloverBootloader/regcomp.c in line 2354 is not initialized when it is used by char_len at CloverBootloader/regcomp.c in line 2354.

	Source	Destination

File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	2414	2453
Object	0	char_len

Code Snippet
File Name CloverBootloader/regcomp.c
Method get_char_len_node1(Node* node, regex_t* reg, int* len, int level)

```
....
2414.            *len = 0;
....
2453.              en->char_len = *len;
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=70
Status	New

The variable declared in 0 at CloverBootloader/regcomp.c in line 5175 is not initialized when it is used by reach_end at CloverBootloader/regcomp.c in line 5175.

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	5208	5208
Object	0	reach_end

Code Snippet
File Name CloverBootloader/regcomp.c
Method concat_opt_exact(OptStr* to, OptStr* add, OnigEncoding enc)

```
....
5208.    to->reach_end = (p == end ? add->reach_end : 0);
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=71
Status	New

The variable declared in 0 at CloverBootloader/regcomp.c in line 5175 is not initialized when it is used by reach_end at CloverBootloader/regcomp.c in line 5175.

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c

Line	5208	5211
Object	0	reach_end

Code Snippet
File Name CloverBootloader/regcomp.c
Method concat_opt_exact(OptStr* to, OptStr* add, OnigEncoding enc)

```
....
5208.    to->reach_end = (p == end ? add->reach_end : 0);
....
5211.    if (! to->reach_end) tanc.right = 0;
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=72
Status	New

The variable declared in os at CloverBootloader/a_bytes.c in line 252 is not initialized when it is used by length at CloverBootloader/a_bytes.c in line 252.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	254	298
Object	os	length

Code Snippet
File Name CloverBootloader/a_bytes.c
Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

```
....
254.        ASN1_STRING *os=NULL;
....
298.              num+=os->length;
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=73
Status	New

The variable declared in os at CloverBootloader/a_bytes.c in line 252 is not initialized when it is used by length at CloverBootloader/a_bytes.c in line 252.

	Source	Destination

File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	254	290
Object	os	length

Code Snippet
File Name CloverBootloader/a_bytes.c
Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

```
....
254.        ASN1_STRING *os=NULL;
....
290.              if (!BUF_MEM_grow_clean(&b,num+os->length))
```

NULL Pointer Dereference\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=74
Status New

The variable declared in os at CloverBootloader/a_bytes.c in line 252 is not initialized when it is used by length at CloverBootloader/a_bytes.c in line 252.

	Source	Destination
File	CloverBootloader/a_bytes.c	CloverBootloader/a_bytes.c
Line	254	295
Object	os	length

Code Snippet
File Name CloverBootloader/a_bytes.c
Method static int asn1_collate_primitive(ASN1_STRING *a, ASN1_const_CTX *c)

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

NULL Pointer Dereference\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=75
Status New

The variable declared in b at CloverBootloader/a_d2i_fp.c in line 87 is not initialized when it is used by data at CloverBootloader/a_d2i_fp.c in line 87.

	Source	Destination
File	CloverBootloader/a_d2i_fp.c	CloverBootloader/a_d2i_fp.c
Line	89	97
Object	b	data

Code Snippet
File Name CloverBootloader/a_d2i_fp.c
Method void *ASN1_d2i_bio(void *(*xnew)(void), d2i_of_void *d2i, BIO *in, void **x)

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

NULL Pointer Dereference\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=76
Status New

The variable declared in b at CloverBootloader/a_d2i_fp.c in line 106 is not initialized when it is used by data at CloverBootloader/a_d2i_fp.c in line 106.

	Source	Destination
File	CloverBootloader/a_d2i_fp.c	CloverBootloader/a_d2i_fp.c
Line	108	116
Object	b	data

Code Snippet
File Name CloverBootloader/a_d2i_fp.c
Method void *ASN1_item_d2i_bio(const ASN1_ITEM *it, BIO *in, void *x)

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

NULL Pointer Dereference\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=77
Status New

The variable declared in ri at CloverBootloader/cms_env.c in line 147 is not initialized when it is used by type at CloverBootloader/cms_env.c in line 147.

	Source	Destination
File	CloverBootloader/cms_env.c	CloverBootloader/cms_env.c
Line	150	169
Object	ri	type

Code Snippet
File Name CloverBootloader/cms_env.c
Method CMS_RecipientInfo *CMS_add1_recipient_cert(CMS_ContentInfo *cms,

```
....
150.        CMS_RecipientInfo *ri = NULL;
....
169.        ri->type = CMS_RECIPINFO_TRANS;
```

NULL Pointer Dereference\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=78
Status New

The variable declared in ri at CloverBootloader/cms_env.c in line 147 is not initialized when it is used by ktri at CloverBootloader/cms_env.c in line 147.

	Source	Destination
File	CloverBootloader/cms_env.c	CloverBootloader/cms_env.c
Line	150	166
Object	ri	ktri

Code Snippet
File Name CloverBootloader/cms_env.c
Method CMS_RecipientInfo *CMS_add1_recipient_cert(CMS_ContentInfo *cms,

```
....
150.        CMS_RecipientInfo *ri = NULL;
....
166.        ri->d.ktri = M_ASN1_new_of(CMS_KeyTransRecipientInfo);
```

NULL Pointer Dereference\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=79
Status New

The variable declared in ri at CloverBootloader/cms_env.c in line 147 is not initialized when it is used by d at CloverBootloader/cms_env.c in line 147.

	Source	Destination
File	CloverBootloader/cms_env.c	CloverBootloader/cms_env.c
Line	150	167
Object	ri	d

Code Snippet
File Name CloverBootloader/cms_env.c
Method CMS_RecipientInfo *CMS_add1_recipient_cert(CMS_ContentInfo *cms,

```
....
150.        CMS_RecipientInfo *ri = NULL;
....
167.        if (!ri->d.ktri)
```

NULL Pointer Dereference\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=80
Status New

The variable declared in ri at CloverBootloader/cms_env.c in line 147 is not initialized when it is used by d at CloverBootloader/cms_env.c in line 147.

	Source	Destination
File	CloverBootloader/cms_env.c	CloverBootloader/cms_env.c
Line	150	171
Object	ri	d

Code Snippet
File Name CloverBootloader/cms_env.c
Method CMS_RecipientInfo *CMS_add1_recipient_cert(CMS_ContentInfo *cms,

```
....
150.        CMS_RecipientInfo *ri = NULL;
....
171.        ktri = ri->d.ktri;
```

NULL Pointer Dereference\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=81
Status New

The variable declared in ri at CloverBootloader/cms_env.c in line 479 is not initialized when it is used by type at CloverBootloader/cms_env.c in line 479.

	Source	Destination
File	CloverBootloader/cms_env.c	CloverBootloader/cms_env.c
Line	486	545
Object	ri	type

Code Snippet
File Name CloverBootloader/cms_env.c
Method CMS_RecipientInfo *CMS_add0_recipient_key(CMS_ContentInfo *cms, int nid,

```
....
486.        CMS_RecipientInfo *ri = NULL;
....
545.        ri->type = CMS_RECIPINFO_KEK;
```

NULL Pointer Dereference\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=82
Status New

The variable declared in ri at CloverBootloader/cms_env.c in line 479 is not initialized when it is used by kekri at CloverBootloader/cms_env.c in line 479.

	Source	Destination
File	CloverBootloader/cms_env.c	CloverBootloader/cms_env.c
Line	486	542
Object	ri	kekri

Code Snippet
File Name CloverBootloader/cms_env.c
Method CMS_RecipientInfo *CMS_add0_recipient_key(CMS_ContentInfo *cms, int nid,

```
....
486.        CMS_RecipientInfo *ri = NULL;
....
542.        ri->d.kekri = M_ASN1_new_of(CMS_KEKRecipientInfo);
```

NULL Pointer Dereference\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=83
Status New

The variable declared in ri at CloverBootloader/cms_env.c in line 479 is not initialized when it is used by d at CloverBootloader/cms_env.c in line 479.

	Source	Destination
File	CloverBootloader/cms_env.c	CloverBootloader/cms_env.c
Line	486	543
Object	ri	d

Code Snippet
File Name CloverBootloader/cms_env.c
Method CMS_RecipientInfo *CMS_add0_recipient_key(CMS_ContentInfo *cms, int nid,

```
....
486.         CMS_RecipientInfo *ri = NULL;
....
543.         if (!ri->d.kekri)
```

NULL Pointer Dereference\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=84
Status New

The variable declared in ri at CloverBootloader/cms_env.c in line 479 is not initialized when it is used by d at CloverBootloader/cms_env.c in line 479.

	Source	Destination
File	CloverBootloader/cms_env.c	CloverBootloader/cms_env.c
Line	486	547
Object	ri	d

Code Snippet
File Name CloverBootloader/cms_env.c
Method CMS_RecipientInfo *CMS_add0_recipient_key(CMS_ContentInfo *cms, int nid,

```
....
486.         CMS_RecipientInfo *ri = NULL;
....
547.         kekri = ri->d.kekri;
```

NULL Pointer Dereference\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=85
Status New

The variable declared in ret at CloverBootloader/dsa_ossl.c in line 131 is not initialized when it is used by r at CloverBootloader/dsa_ossl.c in line 131.

	Source	Destination
File	CloverBootloader/dsa_ossl.c	CloverBootloader/dsa_ossl.c
Line	138	198
Object	ret	r

Code Snippet
File Name CloverBootloader/dsa_ossl.c
Method static DSA_SIG *dsa_do_sign(const unsigned char *dgst, int dlen, DSA *dsa)

```
....
138.         DSA_SIG *ret=NULL;
....
198.         ret->r = r;
```

NULL Pointer Dereference\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=86
Status New

The variable declared in ret at CloverBootloader/dsa_ossl.c in line 131 is not initialized when it is used by s at CloverBootloader/dsa_ossl.c in line 131.

	Source	Destination
File	CloverBootloader/dsa_ossl.c	CloverBootloader/dsa_ossl.c
Line	138	199
Object	ret	s

Code Snippet
File Name CloverBootloader/dsa_ossl.c
Method static DSA_SIG *dsa_do_sign(const unsigned char *dgst, int dlen, DSA *dsa)

```
....
138.         DSA_SIG *ret=NULL;
....
199.         ret->s = s;
```

NULL Pointer Dereference\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=87
Status New

The variable declared in ret at CloverBootloader/ec_asn1.c in line 570 is not initialized when it is used by cofactor at CloverBootloader/ec_asn1.c in line 570.

	Source	Destination
File	CloverBootloader/ec_asn1.c	CloverBootloader/ec_asn1.c
Line	575	668
Object	ret	cofactor

Code Snippet
File Name CloverBootloader/ec_asn1.c
Method static ECPARAMETERS *ec_asn1_group2parameters(const EC_GROUP *group,

```
....
575.         ECPARAMETERS    *ret=NULL;
....
668.                 ret->cofactor = BN_to_ASN1_INTEGER(tmp, ret-
>cofactor);
```

NULL Pointer Dereference\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=88
Status New

The variable declared in ret at CloverBootloader/ec_asn1.c in line 570 is not initialized when it is used by order at CloverBootloader/ec_asn1.c in line 570.

	Source	Destination
File	CloverBootloader/ec_asn1.c	CloverBootloader/ec_asn1.c
Line	575	658
Object	ret	order

Code Snippet
File Name CloverBootloader/ec_asn1.c
Method static ECPARAMETERS *ec_asn1_group2parameters(const EC_GROUP *group,

```
....
575.         ECPARAMETERS    *ret=NULL;
....
658.         ret->order = BN_to_ASN1_INTEGER(tmp, ret->order);
```

NULL Pointer Dereference\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=89
Status New

The variable declared in ret at CloverBootloader/ec_asn1.c in line 570 is not initialized when it is used by base at CloverBootloader/ec_asn1.c in line 570.

	Source	Destination
File	CloverBootloader/ec_asn1.c	CloverBootloader/ec_asn1.c
Line	575	641
Object	ret	base

Code Snippet
File Name CloverBootloader/ec_asn1.c
Method static ECPARAMETERS *ec_asn1_group2parameters(const EC_GROUP *group,

```
....
575.         ECPARAMETERS    *ret=NULL;
....
641.         if (ret->base == NULL && (ret->base =
ASN1_OCTET_STRING_new()) == NULL)
```

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=1020030&projectid=20025&pathid=141
Status New

	Source	Destination
File	CloverBootloader/bn_gf2m.c	CloverBootloader/bn_gf2m.c
Line	346	346
Object	n	n

Code Snippet
File Name CloverBootloader/bn_gf2m.c
Method int BN_GF2m_mod_arr(BIGNUM *r, const BIGNUM *a, const int p[])

```
....
346.                     z[n] ^= (zz << d0);
```

Unchecked Array Index\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=142

Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	728	728
Object	byte_len	byte_len

Code Snippet
File Name CloverBootloader/regcomp.c
Method add_compile_string(UChar* s, int mb_len, int str_len,

```
....
728.      COP(reg)->exact.s[byte_len] = '\0';
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=143
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	2036	2036
Object	j	j

Code Snippet
File Name CloverBootloader/regcomp.c
Method compile_tree(Node* node, regex_t* reg, ScanEnv* env)

```
....
2036.                ns[j] = p[i];
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=144
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	2166	2166
Object	pos	pos

Code Snippet	
File Name	CloverBootloader/regcomp.c
Method	renumber_node_backref(Node* node, GroupNumRemap* map)

```
....
2166.        backs[pos] = n;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=145
Status	New

	Source	Destination
File	CloverBootloader/regcomp.c	CloverBootloader/regcomp.c
Line	2304	2304
Object	pos	pos

Code Snippet	
File Name	CloverBootloader/regcomp.c
Method	disable_noname_group_capture(Node** root, regex_t* reg, ScanEnv* env)

```
....
2304.        SCANENV_MEMENV(env)[pos] = SCANENV_MEMENV(env)[i];
```

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=1020030&projectid=20025&pathid=3
Status	New

The PrintMessage method calls the sprintf function, at line 362 of CloverBootloader/EfiUtilityMsgs.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	CloverBootloader/EfiUtilityMsgs.c	CloverBootloader/EfiUtilityMsgs.c

Line	462	462
Object	sprintf	sprintf

Code Snippet
File Name CloverBootloader/EfiUtilityMsgs.c
Method PrintMessage (

```
....
462.          sprintf (Line2, "(%u)", (unsigned) LineNumber);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=4
Status	New

The PrintMessage method calls the sprintf function, at line 362 of CloverBootloader/EfiUtilityMsgs.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	CloverBootloader/EfiUtilityMsgs.c	CloverBootloader/EfiUtilityMsgs.c
Line	477	477
Object	sprintf	sprintf

Code Snippet
File Name CloverBootloader/EfiUtilityMsgs.c
Method PrintMessage (

```
....
477.          sprintf (Line2, "(%u)", (unsigned) LineNumber);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=5
Status	New

The PrintMessage method calls the sprintf function, at line 362 of CloverBootloader/EfiUtilityMsgs.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	CloverBootloader/EfiUtilityMsgs.c	CloverBootloader/EfiUtilityMsgs.c

Line	504	504
Object	sprintf	sprintf

Code Snippet
File Name CloverBootloader/EfiUtilityMsgs.c
Method PrintMessage (

```
....
504.      sprintf (Line2, " %04u", (unsigned) MessageCode);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=6
Status	New

The main method calls the buf function, at line 55 of CloverBootloader/main.cpp. 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	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	136	136
Object	buf	buf

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
136.    char* buf = (char*)malloc(st.st_size+1);
```

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=1020030&projectid=20025&pathid=8
Status	New

The buffer allocated by <= in CloverBootloader/e_aes.c at line 589 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	CloverBootloader/e_aes.c	CloverBootloader/e_aes.c
Line	598	598
Object	<=	<=

Code Snippet
File Name CloverBootloader/e_aes.c
Method static int aes_ecb_cipher(EVP_CIPHER_CTX *ctx,unsigned char *out,

```
....
598.        for (i=0,len-=bl;i<=len;i+=bl)
```

Potential Off by One Error in Loops\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=9
Status New

The buffer allocated by <= in CloverBootloader/obj_dat.c at line 247 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	CloverBootloader/obj_dat.c	CloverBootloader/obj_dat.c
Line	264	264
Object	<=	<=

Code Snippet
File Name CloverBootloader/obj_dat.c
Method int OBJ_add_object(const ASN1_OBJECT *obj)

```
....
264.        for (i=ADDED_DATA; i<=ADDED_NID; 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=1020030&projectid=20025&pathid=10
Status New

The buffer allocated by <= in CloverBootloader/obj_dat.c at line 247 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	CloverBootloader/obj_dat.c	CloverBootloader/obj_dat.c
Line	283	283
Object	<=	<=

Code Snippet
File Name CloverBootloader/obj_dat.c
Method int OBJ_add_object(const ASN1_OBJECT *obj)

```
....
283.        for (i=ADDED_DATA; i<=ADDED_NID; i++)
```

Heuristic 2nd Order Buffer Overflow read

Query Path:
CPP\Cx\CPP Heuristic\Heuristic 2nd Order Buffer Overflow read Version:0

Categories

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

Description

Heuristic 2nd Order Buffer Overflow read\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=119
Status	New

The size of the buffer used by read_all in nbluTotal, at line 28 of CloverBootloader/main.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_all passes to BinaryExpr, at line 28 of CloverBootloader/main.cpp, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	33	33
Object	BinaryExpr	nbluTotal

Code Snippet
File Name CloverBootloader/main.cpp
Method ssize_t read_all(int fd, void* buf, size_t size)

```
....
33.      ssize_t nblu = read(fd, ((uint8_t*)buf)+nbluTotal, MIN(65536,
size-nbluTotal));
```

Heuristic 2nd Order Buffer Overflow read\Path 2:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=120
Status	New

The size of the buffer used by read_all in BinaryExpr, at line 28 of CloverBootloader/main.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_all passes to BinaryExpr, at line 28 of CloverBootloader/main.cpp, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	33	33
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name CloverBootloader/main.cpp
Method ssize_t read_all(int fd, void* buf, size_t size)

```
....
33.      ssize_t nblu = read(fd, ((uint8_t*)buf)+nbluTotal, MIN(65536,
size-nbluTotal));
```

Heuristic 2nd Order Buffer Overflow read\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=121
Status	New

The size of the buffer used by read_all in <, at line 28 of CloverBootloader/main.cpp, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_all passes to BinaryExpr, at line 28 of CloverBootloader/main.cpp, to overwrite the target buffer.

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	33	33
Object	BinaryExpr	<

Code Snippet
File Name CloverBootloader/main.cpp
Method ssize_t read_all(int fd, void* buf, size_t size)

```
....
33.      ssize_t nblu = read(fd, ((uint8_t*)buf)+nbluTotal, MIN(65536,
size-nbluTotal));
```

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=1020030&projectid=20025&pathid=139
Status	New

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	462	462
Object	final	sizeof

Code Snippet
File Name CloverBootloader/evp_enc.c
Method int EVP_DecryptUpdate(EVP_CIPHER_CTX *ctx, unsigned char *out, int *outl,

```
....
462.        OPENSSL_assert(b <= sizeof ctx->final);
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=140
Status	New

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	535	535
Object	final	sizeof

Code Snippet
File Name CloverBootloader/evp_enc.c
Method int EVP_DecryptFinal_ex(EVP_CIPHER_CTX *ctx, unsigned char *out, int *outl)

```
....
535.            OPENSSL_assert(b <= sizeof ctx->final);
```

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=1020030&projectid=20025&pathid=399
Status	New

The system data read by main in the file CloverBootloader/main.cpp at line 55 is potentially exposed by main found in CloverBootloader/main.cpp at line 55.

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	140	140
Object	errno	fprintf

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
140.      fprintf(stderr, "Cannot open file '%s'. Errno %s\n", path,
strerror(errno));
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=400
Status	New

The system data read by main in the file CloverBootloader/main.cpp at line 55 is potentially exposed by main found in CloverBootloader/main.cpp at line 55.

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	145	145
Object	errno	fprintf

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
145.      fprintf(stderr, "Cannot read file '%s'. Errno %s\n", path,
strerror(errno));
```

Inconsistent Implementations

Query Path:
CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1020030&projectid=20025&pathid=2
Status	New

	Source	Destination
File	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	79	79
Object	getopt_long	getopt_long

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
79.      c = getopt_long (argc, argv, "productname:info:hv",
long_options, &option_index);
```

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=1020030&projectid=20025&pathid=401
Status	New

The main method in CloverBootloader/main.cpp 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	CloverBootloader/main.cpp	CloverBootloader/main.cpp
Line	138	138
Object	open	open

Code Snippet
File Name CloverBootloader/main.cpp
Method extern "C" int main(int argc, char * const argv[])

```
....
138.    int fd = open(path, O_RDONLY);
```

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=1020030&projectid=20025&pathid=402
Status	New

	Source	Destination
File	CloverBootloader/evp_enc.c	CloverBootloader/evp_enc.c
Line	84	84
Object	cipher=	cipher=

Code Snippet
File Name CloverBootloader/evp_enc.c
Method /* ctx->cipher=NULL; */

```
....
84.   /* ctx->cipher=NULL; */
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

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

Cause

How does it happen

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

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

General Recommendations

How to avoid it

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

Source Code Examples

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

---

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
	int i;
	i = 1;
	return &i;
}

void func2()
```

```
{
	int j;
	j = 5;
}

//..
	int * i = func1();
	printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
	func2();
	printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

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

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

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

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

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

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;
}
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged 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 senstiive 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

```
/* Pesumably 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**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Uninitialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Use of 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());
```

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);
}
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

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 Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

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
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Heuristic 2nd Order Buffer Overflow read

Risk

What might happen

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

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

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

Source Code Examples

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-10-29	Unchecked Array Indexing

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	7 Pernicious Kingdoms		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Missing or Inconsistent Access Control

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
           incrementCounter ic;
           decrementCounter dc;
           while(counter == 0) { // because of proper locking, this condition is never false
                  counter = 0;
                  ic = new incrementCounter();
                  dc = new decrementCounter();
                  ic.start();
                  dc.start();
                  ic.join();
                  dc.join();
           }
           System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter--;
           }
        }
    }
```

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

Scanned Languages

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