darktable Scan Report

Project Name	darktable
Scan Start	Friday, June 21, 2024 11:42:35 PM
Preset	Checkmarx Default
Scan Time	00h:03m:11s
Lines Of Code Scanned	20406
Files Scanned	17
Report Creation Time	Friday, June 21, 2024 11:57:56 PM
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	1/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

Uncategorized	All
Custom	All
PCI DSS v3.2	All
OWASP Top 10 2013	All
FISMA 2014	All
NIST SP 800-53	All
OWASP Top 10 2017	All
OWASP Mobile Top 10 2016	All

Excluded:

Uncategorized	None
Custom	None
PCI DSS v3.2	None
OWASP Top 10 2013	None
FISMA 2014	None

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

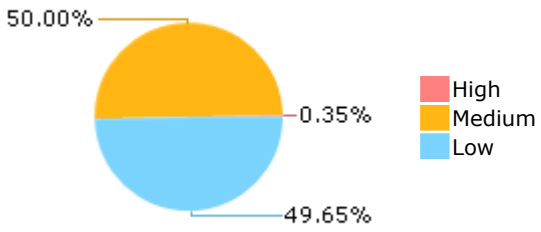
Results Limit

Results limit per query was set to 50

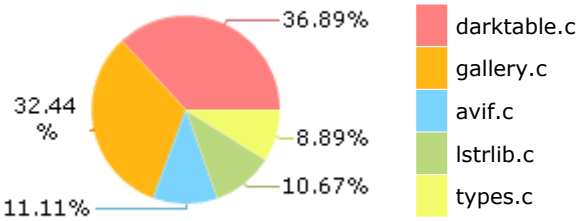
Selected Queries

Selected queries are listed in Result Summary

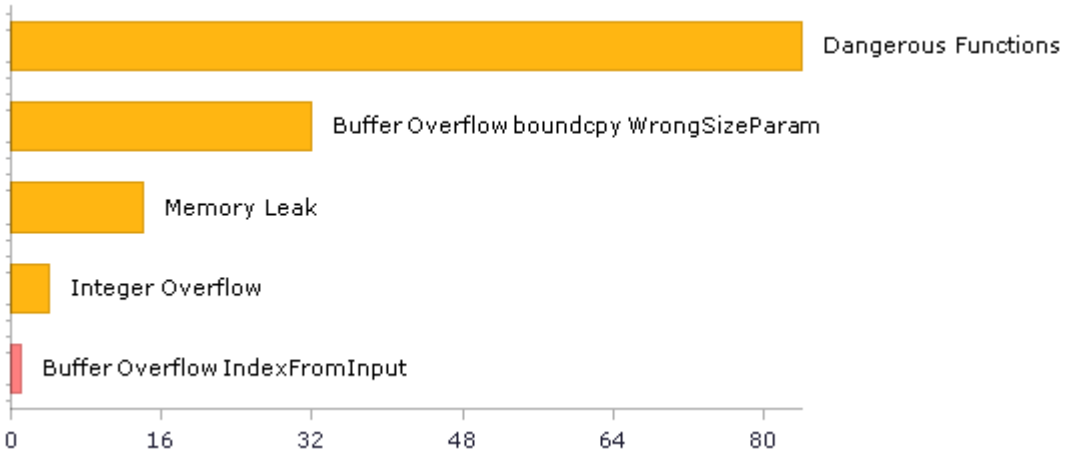
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2017

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	57	38
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	14	14
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	84	84
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	84	84
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	36	36
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.	2	2
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	14	14
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	4	4

***** 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)	14	14
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	41	22
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	46	46
SI-11 Error Handling (P2)*	52	52
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	0	0

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

Scan Summary - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it 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

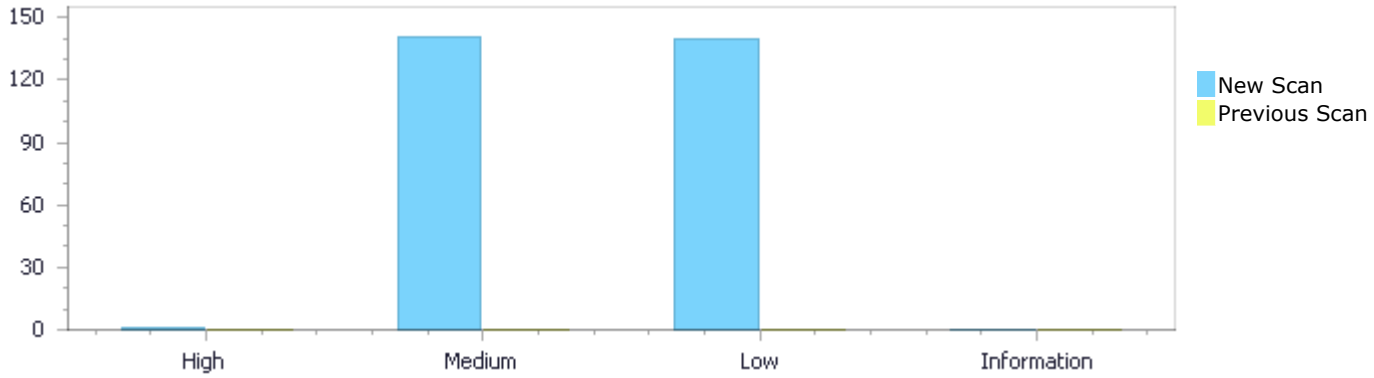
Scan Summary - Custom

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	141	140	0	282
Recurrent Issues	0	0	0	0	0
Total	1	141	140	0	282
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	141	140	0	282
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	1	141	140	0	282

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow IndexFromInput	1	High
Dangerous Functions	84	Medium
Buffer Overflow boundcpy WrongSizeParam	32	Medium
Memory Leak	14	Medium
Integer Overflow	4	Medium

MemoryFree on StackVariable	3	Medium
Use of Zero Initialized Pointer	3	Medium
Wrong Size t Allocation	1	Medium
Unchecked Return Value	52	Low
Unchecked Array Index	39	Low
NULL Pointer Dereference	21	Low
Improper Resource Access Authorization	14	Low
Use of Sizeof On a Pointer Type	8	Low
Potential Precision Problem	3	Low
Arithmenic Operation On Boolean	2	Low
Unreleased Resource Leak	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
darktable/gallery.c	37
darktable/darktable.c	23
darktable/lstrlib.c	21
darktable/lobject.c	16
darktable/conf.c	12
darktable/types.c	11
darktable/mipmap_cache.c	10
darktable/lvm.c	6
darktable/ldo.c	3
darktable/avif.c	3

Scan Results Details

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=282
Status	New

The size of the buffer used by *_sanitize_confgen in n, at line 344 of darktable/conf.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *dt_conf_read_values passes to line, at line 421 of darktable/conf.c, to overwrite the target buffer.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	439	404
Object	line	n

Code Snippet
File Name darktable/conf.c
Method gchar *dt_conf_read_values(const char *filename,

```
....
439.        const char* ret = fgets(line, LINE_SIZE, f);
```

File Name darktable/conf.c
Method static char *_sanitize_confgen(const char *name, const char *value)

```
....
404.          if(!g_ascii_strncasecmp(value, v, n) && v[n] == ']')
```

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=1050079&projectid=50069&pathid=167
Status	New

The dangerous function, memcpy, was found in use at line 191 in darktable/ldo.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/ldo.c	darktable/ldo.c
Line	204	204
Object	memcpy	memcpy

Code Snippet
File Name darktable/ldo.c
Method int luaD_reallocstack (lua_State *L, int newsize, int raiseerror) {

```
....
204.    memcpy(newstack, L->stack, i * sizeof(StackValue));
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=168
Status	New

The dangerous function, memcpy, was found in use at line 557 in darktable/lobject.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	561	561
Object	memcpy	memcpy

Code Snippet
File Name darktable/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
561.        memcpy(out, source + 1, srclen * sizeof(char));
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=169
Status	New

The dangerous function, memcpy, was found in use at line 557 in darktable/lobject.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	569	569
Object	memcpy	memcpy

Code Snippet
File Name darktable/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
569.        memcpy(out, source + 1, srclen * sizeof(char));
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=170
Status	New

The dangerous function, memcpy, was found in use at line 557 in darktable/lobject.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	573	573
Object	memcpy	memcpy

Code Snippet
File Name darktable/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
573.        memcpy(out, source + 1 + srclen - bufflen, bufflen *
sizeof(char));
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=500

	69&pathid=171
Status	New

The dangerous function, memcpy, was found in use at line 557 in darktable/lobject.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	589	589
Object	memcpy	memcpy

Code Snippet
File Name darktable/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
589.      memcpy(out, POS, (LL(POS) + 1) * sizeof(char));
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=172
Status	New

The dangerous function, memcpy, was found in use at line 443 in darktable/lobject.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	446	446
Object	memcpy	memcpy

Code Snippet
File Name darktable/lobject.c
Method static void addstr2buff (BuffFS *buff, const char *str, size_t slen) {

```
....
446.      memcpy(bf, str, slen);  /* add string to buffer */
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=173
Status	New

The dangerous function, memcpy, was found in use at line 150 in darktable/lstrlib.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	164	164
Object	memcpy	memcpy

Code Snippet
File Name darktable/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
164.        memcpy(p, s, l * sizeof(char)); p += l;
```

Dangerous Functions\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=174
Status New

The dangerous function, memcpy, was found in use at line 150 in darktable/lstrlib.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	166	166
Object	memcpy	memcpy

Code Snippet
File Name darktable/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
166.          memcpy(p, sep, lsep * sizeof(char));
```

Dangerous Functions\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=175
Status New

The dangerous function, memcpy, was found in use at line 150 in darktable/lstrlib.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	170	170
Object	memcpy	memcpy

Code Snippet
File Name darktable/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
170.      memcpy(p, s, l * sizeof(char));  /* last copy (not followed by
separator) */
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=176
Status	New

The dangerous function, memcpy, was found in use at line 1192 in darktable/lstrlib.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	1207	1207
Object	memcpy	memcpy

Code Snippet
File Name darktable/lstrlib.c
Method static const char *scanformat (lua_State *L, const char *strfrmt, char *form) {

```
....
1207.    memcpy(form, strfrmt, ((p - strfrmt) + 1) * sizeof(char));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=177
Status	New

The dangerous function, memcpy, was found in use at line 1532 in darktable/lstrlib.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	darktable/lstrlib.c	darktable/lstrlib.c
Line	1535	1535
Object	memcpy	memcpy

Code Snippet
File Name darktable/lstrlib.c
Method static void copywithendian (char *dest, const char *src,

```
....
1535.       memcpy(dest, src, size);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=178
Status	New

The dangerous function, memcpy, was found in use at line 1129 in darktable/lvm.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lvm.c	darktable/lvm.c
Line	1769	1769
Object	memcpy	memcpy

Code Snippet
File Name darktable/lvm.c
Method void luaV_execute (lua_State *L, CallInfo *ci) {

```
....
1769.           memcpy(ra + 4, ra, 3 * sizeof(*ra));
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=179
Status	New

The dangerous function, memcpy, was found in use at line 624 in darktable/lvm.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lvm.c	darktable/lvm.c
Line	628	628

Object	memcpy	memcpy

Code Snippet
File Name darktable/lvm.c
Method static void copy2buff (StkId top, int n, char *buff) {

```
....
628.      memcpy(buff + tl, svalue(s2v(top - n)), l * sizeof(char));
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=180
Status	New

The dangerous function, memcpy, was found in use at line 111 in darktable/mipmap_cache.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	130	130
Object	memcpy	memcpy

Code Snippet
File Name darktable/mipmap_cache.c
Method static inline void dead_image_8(dt_mipmap_buffer_t *buf)

```
....
130.    memcpy(buf->buf, image, sizeof(uint32_t) * 64);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=181
Status	New

The dangerous function, memcpy, was found in use at line 133 in darktable/mipmap_cache.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	155	155
Object	memcpy	memcpy

Code Snippet	
File Name	darktable/mipmap_cache.c
Method	static inline void dead_image_f(dt_mipmap_buffer_t *buf)

```
....
155.    memcpy(buf->buf, image, sizeof(image));
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=182
Status	New

The dangerous function, memcpy, was found in use at line 1138 in darktable/mipmap_cache.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	1144	1144
Object	memcpy	memcpy

Code Snippet	
File Name	darktable/mipmap_cache.c
Method	static int _write_image(dt_imageio_module_data_t *data, const char *filename, const void *in,

```
....
1144.    memcpy(d->buf, in, sizeof(uint32_t) * data->width * data->height);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=183
Status	New

The dangerous function, memcpy, was found in use at line 317 in darktable/types.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	325	325
Object	memcpy	memcpy

Code Snippet

File Name	darktable/types.c
Method	static int full_pushfunc(lua_State *L, luaA_Type type_id, const void *cin)

```
....
325.      memcpy(udata, cin, type_size);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=184
Status	New

The dangerous function, memcpy, was found in use at line 342 in darktable/types.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	350	350
Object	memcpy	memcpy

Code Snippet	
File Name	darktable/types.c
Method	static void full_tofunc(lua_State *L, luaA_Type type_id, void *cout, int index)

```
....
350.    memcpy(cout, udata, luaA_typesize(L, type_id));
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=185
Status	New

The dangerous function, memcpy, was found in use at line 382 in darktable/types.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	390	390
Object	memcpy	memcpy

Code Snippet	
File Name	darktable/types.c
Method	static void int_tofunc(lua_State *L, luaA_Type type_id, void *cout, int index)

```
....
390.    memcpy(cout, udata, sizeof(int));
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=186
Status	New

The dangerous function, memcpy, was found in use at line 425 in darktable/types.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	433	433
Object	memcpy	memcpy

Code Snippet

File Name darktable/types.c

Method static void gpointer_tofunc(lua_State *L, luaA_Type type_id, void *cout, int index)

```
....
433.    memcpy(cout, udata, sizeof(gpointer));
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=187
Status	New

The dangerous function, sprintf, was found in use at line 195 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	265	265
Object	sprintf	sprintf

Code Snippet

File Name darktable/gallery.c

Method int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
265.    sprintf(c, ".%s", ext);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=188
Status	New

The dangerous function, sprintf, was found in use at line 195 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	300	300
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
300.    sprintf(c, "-thumb.%s", ext);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=189
Status	New

The dangerous function, sprintf, was found in use at line 195 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	305	305
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
305.    sprintf(sc, "/img_%d.html", num);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=190
Status	New

The dangerous function, sprintf, was found in use at line 195 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	365	365
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
365.    sprintf(c, "-thumb.%s", ext);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=191
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	391	391
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
391.    sprintf(c, "/style");
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=192
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	393	393
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
393.    sprintf(c, "/style/style.css");
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=193
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	395	395
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
395.    sprintf(c, "/style/favicon.ico");
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=194
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	399	399
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
399.    sprintf(c, "/pswp/default-skin/");
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=195
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	401	401
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
401.    sprintf(c, "/pswp/photoswipe.js");
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=196
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	403	403
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
403.    sprintf(c, "/pswp/photoswipe.min.js");
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=197
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	405	405
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
405.    sprintf(c, "/pswp/photoswipe-ui-default.js");
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=198
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	407	407
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
407.    sprintf(c, "/pswp/photoswipe.css");
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=199
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	409	409
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
409.    sprintf(c, "/pswp/photoswipe-ui-default.min.js");
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=200
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	411	411
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
411.    sprintf(c, "/pswp/default-skin/default-skin.css");
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=201
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	413	413
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
413.    sprintf(c, "/pswp/default-skin/default-skin.png");
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=202
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	415	415
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
415.    sprintf(c, "/pswp/default-skin/default-skin.svg");
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=203
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	417	417
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
417.    sprintf(c, "/pswp/default-skin/preloader.gif");
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=204
Status	New

The dangerous function, sprintf, was found in use at line 383 in darktable/gallery.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	420	420
Object	sprintf	sprintf

Code Snippet

File Name darktable/gallery.c

Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
420.    sprintf(c, "/index.html");
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=205
Status	New

The dangerous function, sscanf, was found in use at line 401 in darktable/darktable.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	416	416
Object	sscanf	sscanf

Code Snippet

File Name darktable/darktable.c

Method void check_resourcelevel(const char *key,

```
....
416.      sscanf(in, "%i %i %i %i", &fractions[g], &fractions[g+1],
&fractions[g+2], &fractions[g+3]);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=206
Status	New

The dangerous function, strcpy, was found in use at line 251 in darktable/lobject.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	263	263
Object	strcpy	strcpy

Code Snippet
File Name darktable/lobject.c
Method static const char *l_str2d (const char *s, lua_Number *result) {

```
....
263.      strcpy(buff, s);  /* copy string to buffer */
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=207
Status	New

The dangerous function, strcpy, was found in use at line 1217 in darktable/lstrlib.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	1221	1221
Object	strcpy	strcpy

Code Snippet
File Name darktable/lstrlib.c
Method static void addlenmod (char *form, const char *lenmod) {

```
....
1221.    strcpy(form + l - 1, lenmod);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=208
Status	New

The dangerous function, strlen, was found in use at line 206 in darktable/avif.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	442	442
Object	strlen	strlen

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
442.    /* TODO: workaround; remove when exiv2 implements AVIF write
support and update flags() */
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=209
Status	New

The dangerous function, strlen, was found in use at line 319 in darktable/conf.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	323	323
Object	strlen	strlen

Code Snippet
File Name darktable/conf.c
Method gboolean dt_conf_key_not_empty(const char *name)

```
....
323.    if(strlen(val) == 0) return FALSE;
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=210
Status	New

The dangerous function, strlen, was found in use at line 344 in darktable/conf.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	400	400
Object	strlen	strlen

Code Snippet
File Name darktable/conf.c
Method static char *_sanitize_confgen(const char *name, const char *value)

```
....
400.        size_t n = strlen(value);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=211
Status	New

The dangerous function, strlen, was found in use at line 421 in darktable/conf.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	444	444
Object	strlen	strlen

Code Snippet
File Name darktable/conf.c
Method gchar *dt_conf_read_values(const char *filename,

```
....
444.          char *end = line + strlen(line);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=212
Status	New

The dangerous function, strlen, was found in use at line 528 in darktable/conf.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	530	530
Object	strlen	strlen

Code Snippet
File Name darktable/conf.c
Method static void _conf_add(char *key, char *val, dt_conf_dreggn_t *d)

```
....
530.    if(strncmp(key, d->match, strlen(d->match)) == 0)
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=213
Status	New

The dangerous function, strlen, was found in use at line 528 in darktable/conf.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	533	533
Object	strlen	strlen

Code Snippet
File Name darktable/conf.c
Method static void _conf_add(char *key, char *val, dt_conf_dreggn_t *d)

```
....
533.      nv->key = g_strdup(key + strlen(d->match) + 1);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=214
Status	New

The dangerous function, strlen, was found in use at line 795 in darktable/conf.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	806	806
Object	strlen	strlen

Code Snippet
File Name darktable/conf.c
Method gchar* dt_conf_expand_default_dir(const char *dir)

```
....
806.      path = g_strdup_printf("%s%s", configdir, dir +
strlen(CONFIG_DIR));
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=215
Status	New

The dangerous function, strlen, was found in use at line 795 in darktable/conf.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	811	811
Object	strlen	strlen

Code Snippet
File Name darktable/conf.c
Method gchar* dt_conf_expand_default_dir(const char *dir)

```
....
811.      path = g_strdup_printf("%s%s", homedir, dir +
strlen(HOME_DIR));
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=216
Status	New

The dangerous function, strlen, was found in use at line 223 in darktable/darktable.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	231	231
Object	strlen	strlen

Code Snippet
File Name darktable/darktable.c
Method gboolean dt_supported_image(const gchar *filename)

```
....
231.      if(!g_ascii_strncasecmp(ext, *i, strlen(*i)))
```

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=1050079&projectid=50069&pathid=61
Status	New

The size of the buffer used by dead_image_f in image, at line 133 of darktable/mipmap_cache.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dead_image_f passes to image, at line 133 of darktable/mipmap_cache.c, to overwrite the target buffer.

	Source	Destination

File	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	155	155
Object	image	image

Code Snippet
File Name darktable/mipmap_cache.c
Method static inline void dead_image_f(dt_mipmap_buffer_t *buf)

```
....
155.    memcpy(buf->buf, image, sizeof(image));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=62
Status	New

The size of the buffer used by int_tofunc in int, at line 382 of darktable/types.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that int_tofunc passes to int, at line 382 of darktable/types.c, to overwrite the target buffer.

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	390	390
Object	int	int

Code Snippet
File Name darktable/types.c
Method static void int_tofunc(lua_State *L, luaA_Type type_id, void *cout, int index)

```
....
390.    memcpy(cout, udata, sizeof(int));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=63
Status	New

The size of the buffer used by gpointer_tofunc in gpointer, at line 425 of darktable/types.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gpointer_tofunc passes to gpointer, at line 425 of darktable/types.c, to overwrite the target buffer.

	Source	Destination
File	darktable/types.c	darktable/types.c

Line	433	433
Object	gpointer	gpointer

Code Snippet
File Name darktable/types.c
Method static void gpointer_tofunc(lua_State *L, luaA_Type type_id, void *cout, int index)

```
....
433.    memcpy(cout, udata, sizeof(gpointer));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=64
Status	New

The size of the buffer used by dt_codepaths_init in Namespace2033313065, at line 310 of darktable/darktable.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dt_codepaths_init passes to Namespace2033313065, at line 310 of darktable/darktable.c, to overwrite the target buffer.

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	316	316
Object	Namespace2033313065	Namespace2033313065

Code Snippet
File Name darktable/darktable.c
Method static void dt_codepaths_init()

```
....
316.    memset(&(darktable.codepath), 0, sizeof(darktable.codepath));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=65
Status	New

The size of the buffer used by dt_init in darktable_t, at line 516 of darktable/darktable.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dt_init passes to darktable_t, at line 516 of darktable/darktable.c, to overwrite the target buffer.

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c

Line	548	548
Object	darktable_t	darktable_t

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
548.    memset(&darktable, 0, sizeof(darktable_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=66
Status	New

The size of the buffer used by dt_lua_init_singleton in void, at line 674 of darktable/types.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dt_lua_init_singleton passes to void, at line 674 of darktable/types.c, to overwrite the target buffer.

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	687	687
Object	void	void

Code Snippet
File Name darktable/types.c
Method luaA_Type dt_lua_init_singleton(lua_State *L, const char *unique_name, void *data)

```
....
687.      memset(udata, 0, sizeof(void *));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=67
Status	New

The size of the buffer used by luaD_reallocstack in i, at line 191 of darktable/ldo.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaD_reallocstack passes to i, at line 191 of darktable/ldo.c, to overwrite the target buffer.

	Source	Destination
File	darktable/ldo.c	darktable/ldo.c

Line	204	204
Object	i	i

Code Snippet
File Name darktable/ldo.c
Method int luaD_reallocstack (lua_State *L, int newsize, int raiseerror) {

```
....
204.    memcpy(newstack, L->stack, i * sizeof(StackValue));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=68
Status	New

The size of the buffer used by luaD_reallocstack in StackValue, at line 191 of darktable/ldo.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaD_reallocstack passes to StackValue, at line 191 of darktable/ldo.c, to overwrite the target buffer.

	Source	Destination
File	darktable/ldo.c	darktable/ldo.c
Line	204	204
Object	StackValue	StackValue

Code Snippet
File Name darktable/ldo.c
Method int luaD_reallocstack (lua_State *L, int newsize, int raiseerror) {

```
....
204.    memcpy(newstack, L->stack, i * sizeof(StackValue));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=69
Status	New

The size of the buffer used by luaO_chunkid in srclen, at line 557 of darktable/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to srclen, at line 557 of darktable/lobject.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	561	561

Object	srclen	srclen

Code Snippet
File Name darktable/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
561.        memcpy(out, source + 1, srclen * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=70
Status	New

The size of the buffer used by luaO_chunkid in char, at line 557 of darktable/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to char, at line 557 of darktable/lobject.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	561	561
Object	char	char

Code Snippet
File Name darktable/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
561.        memcpy(out, source + 1, srclen * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=71
Status	New

The size of the buffer used by luaO_chunkid in srclen, at line 557 of darktable/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to srclen, at line 557 of darktable/lobject.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	569	569
Object	srclen	srclen

Code Snippet
File Name darktable/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
569.        memcpy(out, source + 1, srclen * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=72
Status	New

The size of the buffer used by luaO_chunkid in char, at line 557 of darktable/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to char, at line 557 of darktable/lobject.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	569	569
Object	char	char

Code Snippet
File Name darktable/lobject.c
Method void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
569.        memcpy(out, source + 1, srclen * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=73
Status	New

The size of the buffer used by luaO_chunkid in bufflen, at line 557 of darktable/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to bufflen, at line 557 of darktable/lobject.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	573	573
Object	bufflen	bufflen

Code Snippet
File Name darktable/lobject.c

Method	void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
573.        memcpy(out, source + 1 + srclen - bufflen, bufflen *
sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=74
Status	New

The size of the buffer used by luaO_chunkid in char, at line 557 of darktable/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to char, at line 557 of darktable/lobject.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	573	573
Object	char	char

Code Snippet	
File Name	darktable/lobject.c
Method	void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
573.        memcpy(out, source + 1 + srclen - bufflen, bufflen *
sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=75
Status	New

The size of the buffer used by luaO_chunkid in char, at line 557 of darktable/lobject.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaO_chunkid passes to char, at line 557 of darktable/lobject.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	589	589
Object	char	char

Code Snippet	
File Name	darktable/lobject.c
Method	void luaO_chunkid (char *out, const char *source, size_t srclen) {

```
....
589.      memcpy(out, POS, (LL(POS) + 1) * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=76
Status	New

The size of the buffer used by str_rep in l, at line 150 of darktable/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that str_rep passes to l, at line 150 of darktable/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	164	164
Object	l	l

Code Snippet
File Name darktable/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
164.        memcpy(p, s, l * sizeof(char)); p += l;
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=77
Status	New

The size of the buffer used by str_rep in char, at line 150 of darktable/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that str_rep passes to char, at line 150 of darktable/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	164	164
Object	char	char

Code Snippet
File Name darktable/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
164.        memcpy(p, s, l * sizeof(char)); p += l;
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=78
Status	New

The size of the buffer used by str_rep in lsep, at line 150 of darktable/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that str_rep passes to lsep, at line 150 of darktable/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	166	166
Object	lsep	lsep

Code Snippet
File Name darktable/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
166.          memcpy(p, sep, lsep * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=79
Status	New

The size of the buffer used by str_rep in char, at line 150 of darktable/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that str_rep passes to char, at line 150 of darktable/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	166	166
Object	char	char

Code Snippet
File Name darktable/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
166.          memcpy(p, sep, lsep * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=80
Status	New

The size of the buffer used by str_rep in l, at line 150 of darktable/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that str_rep passes to l, at line 150 of darktable/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	170	170
Object	l	l

Code Snippet
File Name darktable/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
170.      memcpy(p, s, l * sizeof(char));  /* last copy (not followed by
separator) */
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=81
Status	New

The size of the buffer used by str_rep in char, at line 150 of darktable/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that str_rep passes to char, at line 150 of darktable/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	170	170
Object	char	char

Code Snippet
File Name darktable/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
170.      memcpy(p, s, l * sizeof(char));  /* last copy (not followed by
separator) */
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=82
Status	New

The size of the buffer used by *scanformat in char, at line 1192 of darktable/lstrlib.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *scanformat passes to char, at line 1192 of darktable/lstrlib.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	1207	1207
Object	char	char

Code Snippet
File Name darktable/lstrlib.c
Method static const char *scanformat (lua_State *L, const char *strfrmt, char *form) {

```
....
1207.    memcpy(form, strfrmt, ((p - strfrmt) + 1) * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=83
Status	New

The size of the buffer used by luaV_execute in ra, at line 1129 of darktable/lvm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that luaV_execute passes to ra, at line 1129 of darktable/lvm.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lvm.c	darktable/lvm.c
Line	1769	1769
Object	ra	ra

Code Snippet
File Name darktable/lvm.c
Method void luaV_execute (lua_State *L, CallInfo *ci) {

```
....
1769.          memcpy(ra + 4, ra, 3 * sizeof(*ra));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=84
Status	New

The size of the buffer used by copy2buff in l, at line 624 of darktable/lvm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that copy2buff passes to l, at line 624 of darktable/lvm.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lvm.c	darktable/lvm.c
Line	628	628
Object	l	l

Code Snippet
File Name darktable/lvm.c
Method static void copy2buff (StkId top, int n, char *buff) {

```
....
628.      memcpy(buff + tl, svalue(s2v(top - n)), l * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=85
Status	New

The size of the buffer used by copy2buff in char, at line 624 of darktable/lvm.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that copy2buff passes to char, at line 624 of darktable/lvm.c, to overwrite the target buffer.

	Source	Destination
File	darktable/lvm.c	darktable/lvm.c
Line	628	628
Object	char	char

Code Snippet
File Name darktable/lvm.c
Method static void copy2buff (StkId top, int n, char *buff) {

```
....
628.      memcpy(buff + tl, svalue(s2v(top - n)), l * sizeof(char));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=86
Status	New

The size of the buffer used by dead_image_8 in uint32_t, at line 111 of darktable/mipmap_cache.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dead_image_8 passes to uint32_t, at line 111 of darktable/mipmap_cache.c, to overwrite the target buffer.

	Source	Destination
File	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	130	130
Object	uint32_t	uint32_t

Code Snippet
File Name darktable/mipmap_cache.c
Method static inline void dead_image_8(dt_mipmap_buffer_t *buf)

```
....
130.    memcpy(buf->buf, image, sizeof(uint32_t) * 64);
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=87
Status	New

The size of the buffer used by _write_image in data, at line 1138 of darktable/mipmap_cache.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _write_image passes to data, at line 1138 of darktable/mipmap_cache.c, to overwrite the target buffer.

	Source	Destination
File	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	1144	1144
Object	data	data

Code Snippet
File Name darktable/mipmap_cache.c
Method static int _write_image(dt_imageio_module_data_t *data, const char *filename, const void *in,

```
....
1144.    memcpy(d->buf, in, sizeof(uint32_t) * data->width * data-
>height);
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=88
Status	New

The size of the buffer used by _write_image in data, at line 1138 of darktable/mipmap_cache.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _write_image passes to data, at line 1138 of darktable/mipmap_cache.c, to overwrite the target buffer.

	Source	Destination
File	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	1144	1144
Object	data	data

Code Snippet
File Name darktable/mipmap_cache.c
Method static int _write_image(dt_imageio_module_data_t *data, const char *filename, const void *in,

```
....
1144.    memcpy(d->buf, in, sizeof(uint32_t) * data->width * data-
>height);
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=89
Status	New

The size of the buffer used by _write_image in uint32_t, at line 1138 of darktable/mipmap_cache.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _write_image passes to uint32_t, at line 1138 of darktable/mipmap_cache.c, to overwrite the target buffer.

	Source	Destination
File	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	1144	1144
Object	uint32_t	uint32_t

Code Snippet
File Name darktable/mipmap_cache.c

Method	static int _write_image(dt_imageio_module_data_t *data, const char *filename, const void *in,

```
....
1144.    memcpy(d->buf, in, sizeof(uint32_t) * data->width * data->height);
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=90
Status	New

The size of the buffer used by full_pushfunc in type_size, at line 317 of darktable/types.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that full_pushfunc passes to type_size, at line 317 of darktable/types.c, to overwrite the target buffer.

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	325	325
Object	type_size	type_size

Code Snippet	
File Name	darktable/types.c
Method	static int full_pushfunc(lua_State *L, luaA_Type type_id, const void *cin)

```
....
325.      memcpy(udata, cin, type_size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=91
Status	New

The size of the buffer used by full_pushfunc in type_size, at line 317 of darktable/types.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that full_pushfunc passes to type_size, at line 317 of darktable/types.c, to overwrite the target buffer.

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	329	329
Object	type_size	type_size

Code Snippet	
File Name	darktable/types.c
Method	static int full_pushfunc(lua_State *L, luaA_Type type_id, const void *cin)

```
....
329.      memset(udata, 0, type_size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=92
Status	New

The size of the buffer used by to_char_array in size, at line 31 of darktable/types.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that to_char_array passes to size, at line 31 of darktable/types.c, to overwrite the target buffer.

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	39	39
Object	size	size

Code Snippet
File Name darktable/types.c
Method static void to_char_array(lua_State *L, luaA_Type type_id, void *c_out, int index, int size)

```
....
39.    strncpy(c_out, value, size);
```

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=1050079&projectid=50069&pathid=251
Status	New

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	597	597
Object	d	d

Code Snippet
File Name darktable/avif.c
Method

```
....
597.  {
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=252
Status	New

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	743	743
Object	gui	gui

Code Snippet
File Name darktable/avif.c
Method static void quality_changed(GtkWidget *slider, gpointer user_data)

```
....
743.    const uint32_t quality = (int)dt_bauhaus_slider_get(slider);
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=253
Status	New

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	147	147
Object	d	d

Code Snippet
File Name darktable/gallery.c
Method void gui_init(dt_imageio_module_storage_t *self)

```
....
147.    gallery_t *d = (gallery_t *)malloc(sizeof(gallery_t));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=254
Status	New

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	542	542
Object	d	d

Code Snippet
File Name darktable/gallery.c
Method void *get_params(dt_imageio_module_storage_t *self)

```
....
542.    dt_imageio_gallery_t *d = (dt_imageio_gallery_t *)calloc(1,
sizeof(dt_imageio_gallery_t));
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=255
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	571	571
Object	control	control

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
571.    darktable.control = (dt_control_t *)calloc(1,
sizeof(dt_control_t));
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=256
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	1140	1140
Object	conf	conf

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1140.    darktable.conf = (dt_conf_t *)calloc(1, sizeof(dt_conf_t));
```

Memory Leak\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=257
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	1255	1255
Object	gui	gui

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1255.      darktable.gui = (dt_gui_gtk_t *)calloc(1,
sizeof(dt_gui_gtk_t));
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=258
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	1340	1340

Object	opencl	opencl

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1340.    darktable.opencl = (dt_opencl_t *)calloc(1,
sizeof(dt_opencl_t));
```

Memory Leak\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=259
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	1346	1346
Object	points	points

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1346.    darktable.points = (dt_points_t *)calloc(1,
sizeof(dt_points_t));
```

Memory Leak\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=260
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	1355	1355
Object	image_cache	image_cache

Code Snippet
File Name darktable/darktable.c

Method	int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1355.    darktable.image_cache = (dt_image_cache_t *)calloc(1,
sizeof(dt_image_cache_t));
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=261
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	1358	1358
Object	mipmap_cache	mipmap_cache

Code Snippet	
File Name	darktable/darktable.c
Method	int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1358.    darktable.mipmap_cache = (dt_mipmap_cache_t *)calloc(1,
sizeof(dt_mipmap_cache_t));
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=262
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	1377	1377
Object	view_manager	view_manager

Code Snippet	
File Name	darktable/darktable.c
Method	int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1377.    darktable.view_manager = (dt_view_manager_t *)calloc(1,
sizeof(dt_view_manager_t));
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=263
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	1388	1388
Object	imageio	imageio

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1388.    darktable.imageio = (dt_imageio_t *)calloc(1,
sizeof(dt_imageio_t));
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=264
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	1432	1432
Object	lib	lib

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1432.      darktable.lib = (dt_lib_t *)calloc(1, sizeof(dt_lib_t));
```

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=1050079&projectid=50069&pathid=122
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 148 of darktable/conf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	176	176
Object	AssignExpr	AssignExpr

Code Snippet
File Name darktable/conf.c
Method int dt_conf_get_int_fast(const char *name)

```
....
176.      val = new_value + 0.5;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=123
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 148 of darktable/conf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	178	178
Object	AssignExpr	AssignExpr

Code Snippet
File Name darktable/conf.c
Method int dt_conf_get_int_fast(const char *name)

```
....
178.      val = new_value - 0.5;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=124
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 177 of darktable/lstrlib.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	187	187
Object	AssignExpr	AssignExpr

Code Snippet
File Name darktable/lstrlib.c
Method static int str_byte (lua_State *L) {

```
....
187.    n = (int)(pose -  posi) + 1;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=125
Status	New

A variable of a larger data type, val, is being assigned to a smaller data type, in 344 of darktable/conf.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	364	364
Object	val	val

Code Snippet
File Name darktable/conf.c
Method static char *_sanitize_confgen(const char *name, const char *value)

```
....
364.        const int val = dt_isnan(v) ? dt_confgen_get_int(name,
DT_DEFAULT) : (int)v;
```

MemoryFree on StackVariable

Query Path:
CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=94
Status	New

Calling free() (line 2064) on a variable that was not dynamically allocated (line 2064) in file darktable/darktable.c may result with a crash.

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	2095	2095
Object	line	line

Code Snippet
File Name darktable/darktable.c
Method void dt_print_mem_usage()

```
....
2095.    free(line);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=95
Status	New

Calling free() (line 345) on a variable that was not dynamically allocated (line 345) in file darktable/darktable.c may result with a crash.

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	364	364
Object	line	line

Code Snippet
File Name darktable/darktable.c
Method static inline size_t _get_total_memory()

```
....
364.    if(len > 0) free(line);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=96
Status	New

Calling free() (line 383) on a variable that was not dynamically allocated (line 383) in file darktable/gallery.c may result with a crash.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	507	507
Object	p	p

Code Snippet

File Name darktable/gallery.c

Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
507.      free(p);
```

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=1050079&projectid=50069&pathid=265
Status	New

The variable declared in noiseprofiles_from_command at darktable/darktable.c in line 516 is not initialized when it is used by noiseprofile_parser at darktable/darktable.c in line 516.

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	575	1351

Object	noiseprofiles_from_command	noiseprofile_parser

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
575.    char *noiseprofiles_from_command = NULL;
....
1351.    darktable.noiseprofile_parser =
dt_noiseprofile_init(noiseprofiles_from_command);
```

Use of Zero Initialized Pointer\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=266
Status New

The variable declared in config_override at darktable/darktable.c in line 516 is not initialized when it is used by config_override at darktable/darktable.c in line 516.

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	602	968
Object	config_override	config_override

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
602.    GSList *config_override = NULL;
....
968.            config_override = g_slist_append(config_override,
entry);
```

Use of Zero Initialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=267
Status New

The variable declared in result at darktable/conf.c in line 540 is not initialized when it is used by result at darktable/conf.c in line 540.

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	544	548
Object	result	result

Code Snippet
File Name darktable/conf.c
Method GSList *dt_conf_all_string_entries(const char *dir)

```
....
544.    d.result = NULL;
....
548.    return d.result;
```

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=1050079&projectid=50069&pathid=97
Status	New

The function aligned_size in darktable/darktable.c at line 1784 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	darktable/darktable.c	darktable/darktable.c
Line	1788	1788
Object	aligned_size	aligned_size

Code Snippet
File Name darktable/darktable.c
Method void *dt_alloc_align(const size_t alignment, const size_t size)

```
....
1788.    return malloc(aligned_size);
```

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=1050079&projectid=50069&pathid=1
Status	New

The dt_print_mem_usage method calls the snprintf function, at line 2064 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	2078	2078
Object	snprintf	snprintf

Code Snippet
File Name darktable/darktable.c
Method void dt_print_mem_usage()

```
....
2078.    snprintf(pidstatus, sizeof(pidstatus), "/proc/%u/status",
(uint32_t)getpid());
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=2
Status	New

The dt_dump_pfm_file method calls the snprintf function, at line 420 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	435	435
Object	snprintf	snprintf

Code Snippet
File Name darktable/darktable.c
Method void dt_dump_pfm_file(

```
....
435.    snprintf(path, sizeof(path), "%s/%s", darktable.tmp_directory,
pipe);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=3
Status	New

The dt_dump_pfm_file method calls the snprintf function, at line 420 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	446	446
Object	snprintf	snprintf

Code Snippet
File Name darktable/darktable.c
Method void dt_dump_pfm_file(

```
....
446.    snprintf(fname, sizeof (fname), "%s/%04d_%s_%s_%s%s.%s",
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=4
Status	New

The dt_init method calls the snprintf function, at line 516 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1137	1137
Object	snprintf	snprintf

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1137.    snprintf(darktablerc, sizeof(darktablerc), "%s/darktablerc",
datadir);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=5
Status	New

The dt_print method calls the snprintf function, at line 1748 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1757	1757
Object	snprintf	snprintf

Code Snippet
File Name darktable/darktable.c
Method void dt_print(dt_debug_thread_t thread, const char *msg, ...)

```
....
1757.    snprintf(buf, sizeof(buf), "%.4f", dt_get_wtime() -
darktable.start_wtime);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=6
Status	New

The *dt_alloc_align method calls the malloc function, at line 1784 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1788	1788
Object	malloc	malloc

Code Snippet
File Name darktable/darktable.c

Method	void *dt_alloc_align(const size_t alignment, const size_t size)

```
....
1788.    return malloc(aligned_size);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=7
Status	New

The dt_show_times method calls the snprintf function, at line 1831 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1840	1840
Object	snprintf	snprintf

Code Snippet	
File Name	darktable/darktable.c
Method	void dt_show_times(const dt_times_t *start, const char *prefix)

```
....
1840.      snprintf(buf, sizeof(buf),
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=8
Status	New

The store method calls the snprintf function, at line 195 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	227	227
Object	snprintf	snprintf

Code Snippet	
File Name	darktable/gallery.c
Method	int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
227.      snprintf(d->filename + strlen(d->filename), sizeof(d-
>filename) - strlen(d->filename), "/$(FILE_NAME)");
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=9
Status	New

The store method calls the snprintf function, at line 195 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	232	232
Object	snprintf	snprintf

Code Snippet
File Name darktable/gallery.c
Method int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
232.      snprintf(d->filename + strlen(d->filename), sizeof(d-
>filename) - strlen(d->filename), "_$(SEQUENCE)");
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=10
Status	New

The store method calls the sprintf function, at line 195 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	265	265
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c

Method	int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
265.    sprintf(c, ".%s", ext);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=11
Status	New

The store method calls the sprintf function, at line 195 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	300	300
Object	sprintf	sprintf

Code Snippet	
File Name	darktable/gallery.c
Method	int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
300.    sprintf(c, "-thumb.%s", ext);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=12
Status	New

The store method calls the sprintf function, at line 195 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	305	305
Object	sprintf	sprintf

Code Snippet	
File Name	darktable/gallery.c

Method	int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
305.    sprintf(sc, "/img_%d.html", num);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=13
Status	New

The store method calls the snprintf function, at line 195 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	306	306
Object	snprintf	snprintf

Code Snippet
File Name darktable/gallery.c
Method int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
306.    snprintf(relsubfilename, sizeof(relsubfilename), "img_%d.html",
num);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=14
Status	New

The store method calls the snprintf function, at line 195 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	313	313
Object	snprintf	snprintf

Code Snippet
File Name darktable/gallery.c

Method	int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
313.    snprintf(pair->line, sizeof(pair->line),
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=15
Status	New

The store method calls the snprintf function, at line 195 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	338	338
Object	snprintf	snprintf

Code Snippet	
File Name	darktable/gallery.c
Method	int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
338.    snprintf(pair->item, sizeof(pair->item),
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=16
Status	New

The store method calls the sprintf function, at line 195 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	365	365
Object	sprintf	sprintf

Code Snippet	
File Name	darktable/gallery.c

Method	int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
365.    sprintf(c, "-thumb.%s", ext);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=17
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	391	391
Object	sprintf	sprintf

Code Snippet	
File Name	darktable/gallery.c
Method	void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
391.    sprintf(c, "/style");
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=18
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	393	393
Object	sprintf	sprintf

Code Snippet

File Name	darktable/gallery.c
Method	void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
393.    sprintf(c, "/style/style.css");
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=19
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	395	395
Object	sprintf	sprintf

Code Snippet

File Name	darktable/gallery.c
Method	void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
395.    sprintf(c, "/style/favicon.ico");
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=20
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	399	399
Object	sprintf	sprintf

Code Snippet	
File Name	darktable/gallery.c
Method	void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
399.    sprintf(c, "/pswp/default-skin/");
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=21
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	401	401
Object	sprintf	sprintf

Code Snippet	
File Name	darktable/gallery.c
Method	void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
401.    sprintf(c, "/pswp/photoswipe.js");
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=22
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	403	403
Object	sprintf	sprintf

Code Snippet	
File Name	darktable/gallery.c
Method	void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
403.    sprintf(c, "/pswp/photoswipe.min.js");
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=23
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	405	405
Object	sprintf	sprintf

Code Snippet	
File Name	darktable/gallery.c
Method	void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
405.    sprintf(c, "/pswp/photoswipe-ui-default.js");
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=24
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	407	407

Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
407.    sprintf(c, "/pswp/photoswipe.css");
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=25
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	409	409
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
409.    sprintf(c, "/pswp/photoswipe-ui-default.min.js");
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=26
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c

Line	411	411
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
411.    sprintf(c, "/pswp/default-skin/default-skin.css");
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=27
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	413	413
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
413.    sprintf(c, "/pswp/default-skin/default-skin.png");
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=28
Status	New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	415	415
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
415.    sprintf(c, "/pswp/default-skin/default-skin.svg");
```

Unchecked Return Value\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=29
Status New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	417	417
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
417.    sprintf(c, "/pswp/default-skin/preloader.gif");
```

Unchecked Return Value\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=30
Status New

The finalize_store method calls the sprintf function, at line 383 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	420	420
Object	sprintf	sprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
420.    sprintf(c, "/index.html");
```

Unchecked Return Value\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=31
Status New

The dt_mipmap_cache_get_filename method calls the snprintf function, at line 187 of darktable/mipmap_cache.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	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	213	213
Object	snprintf	snprintf

Code Snippet
File Name darktable/mipmap_cache.c
Method static int dt_mipmap_cache_get_filename(gchar *mipmapfilename, size_t size)

```
....
213.      snprintf(mipmapfilename, size, "%s/%s", cachedir,
DT_MIPMAP_CACHE_DEFAULT_FILE_NAME);
```

Unchecked Return Value\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=32
Status New

The dt_mipmap_cache_get_filename method calls the snprintf function, at line 187 of darktable/mipmap_cache.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	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	215	215
Object	snprintf	snprintf

Code Snippet
File Name darktable/mipmap_cache.c
Method static int dt_mipmap_cache_get_filename(gchar *mipmapfilename, size_t size)

```
....
215.      snprintf(mipmapfilename, size, "%s/%s-%s", cachedir,
DT_MIPMAP_CACHE_DEFAULT_FILE_NAME, filename);
```

Unchecked Return Value\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=33
Status New

The dt_mipmap_cache_deallocate_dynamic method calls the snprintf function, at line 437 of darktable/mipmap_cache.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	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	456	456
Object	snprintf	snprintf

Code Snippet
File Name darktable/mipmap_cache.c
Method void dt_mipmap_cache_deallocate_dynamic(void *data, dt_cache_entry_t *entry)

```
....
456.          snprintf(filename, sizeof(filename), "%s.d/%d", cache-
>cachedir, mip);
```

Unchecked Return Value\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=34
Status New

The autotype_tostring method calls the snprintf function, at line 298 of darktable/types.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	darktable/types.c	darktable/types.c
Line	307	307
Object	snprintf	snprintf

Code Snippet
File Name darktable/types.c
Method static int autotype_tostring(lua_State *L)

```
....
307.      snprintf(tmp,sizeof(tmp),"%s (%p)",lua_tostring(L,-
1),lua_topointer(L,1));
```

Unchecked Return Value\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=35
Status New

The full_tofunc method calls the snprintf function, at line 342 of darktable/types.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	darktable/types.c	darktable/types.c
Line	346	346
Object	snprintf	snprintf

Code Snippet
File Name darktable/types.c
Method static void full_tofunc(lua_State *L, luaA_Type type_id, void *cout, int index)

```
....
346.      snprintf(error_msg,sizeof(error_msg),"%s
expected",luaA_typename(L,type_id));
```

Unchecked Return Value\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=36
Status New

The int_tofunc method calls the snprintf function, at line 382 of darktable/types.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	darktable/types.c	darktable/types.c
Line	386	386
Object	snprintf	snprintf

Code Snippet
File Name darktable/types.c
Method static void int_tofunc(lua_State *L, luaA_Type type_id, void *cout, int index)

```
....
386.      snprintf(error_msg,sizeof(error_msg),"%s
expected",luaA_typename(L,type_id));
```

Unchecked Return Value\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=37
Status New

The gpointer_tofunc method calls the snprintf function, at line 425 of darktable/types.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	darktable/types.c	darktable/types.c
Line	429	429
Object	snprintf	snprintf

Code Snippet
File Name darktable/types.c
Method static void gpointer_tofunc(lua_State *L, luaA_Type type_id, void *cout, int index)

```
....
429.      snprintf(error_msg,sizeof(error_msg),"%s
expected",luaA_typename(L,type_id));
```

Unchecked Return Value\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=38
Status New

The dt_lua_init_singleton method calls the snprintf function, at line 674 of darktable/types.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	darktable/types.c	darktable/types.c
Line	677	677
Object	snprintf	snprintf

Code Snippet
File Name darktable/types.c
Method luaA_Type dt_lua_init_singleton(lua_State *L, const char *unique_name, void *data)

```
....
677.    snprintf(tmp_name, sizeof(tmp_name), "dt_lua_singleton_%s",
unique_name);
```

Unchecked Return Value\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=39
Status New

The dt_init method calls the control function, at line 516 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	571	571
Object	control	control

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
571.    darktable.control = (dt_control_t *)calloc(1,
sizeof(dt_control_t));
```

Unchecked Return Value\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=500

	69&pathid=40
Status	New

The dt_init method calls the conf function, at line 516 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1140	1140
Object	conf	conf

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1140.    darktable.conf = (dt_conf_t *)calloc(1, sizeof(dt_conf_t));
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=41
Status	New

The dt_init method calls the opencl function, at line 516 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1340	1340
Object	opencl	opencl

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1340.    darktable.opencl = (dt_opencl_t *)calloc(1,
sizeof(dt_opencl_t));
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=500

	69&pathid=42
Status	New

The dt_init method calls the points function, at line 516 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1346	1346
Object	points	points

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1346.    darktable.points = (dt_points_t *)calloc(1,
sizeof(dt_points_t));
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=43
Status	New

The dt_init method calls the image_cache function, at line 516 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1355	1355
Object	image_cache	image_cache

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1355.    darktable.image_cache = (dt_image_cache_t *)calloc(1,
sizeof(dt_image_cache_t));
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=44
Status	New

The dt_init method calls the mipmap_cache function, at line 516 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1358	1358
Object	mipmap_cache	mipmap_cache

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1358.    darktable.mipmap_cache = (dt_mipmap_cache_t *)calloc(1,
sizeof(dt_mipmap_cache_t));
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=45
Status	New

The dt_init method calls the view_manager function, at line 516 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1377	1377
Object	view_manager	view_manager

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1377.    darktable.view_manager = (dt_view_manager_t *)calloc(1,
sizeof(dt_view_manager_t));
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=46
Status	New

The dt_init method calls the imageio function, at line 516 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1388	1388
Object	imageio	imageio

Code Snippet

File Name darktable/darktable.c

Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1388.    darktable.imageio = (dt_imageio_t *)calloc(1,
sizeof(dt_imageio_t));
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=47
Status	New

The dt_init method calls the lib function, at line 516 of darktable/darktable.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	darktable/darktable.c	darktable/darktable.c
Line	1432	1432
Object	lib	lib

Code Snippet

File Name darktable/darktable.c

Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
1432.      darktable.lib = (dt_lib_t *)calloc(1, sizeof(dt_lib_t));
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=48
Status	New

The quality_changed method calls the gui function, at line 741 of darktable/avif.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	darktable/avif.c	darktable/avif.c
Line	743	743
Object	gui	gui

Code Snippet
File Name darktable/avif.c
Method static void quality_changed(GtkWidget *slider, gpointer user_data)

```
....
743.    const uint32_t quality = (int)dt_bauhaus_slider_get(slider);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=49
Status	New

The *legacy_params method calls the n function, at line 76 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	91	91
Object	n	n

Code Snippet
File Name darktable/gallery.c
Method void *legacy_params(dt_imageio_module_storage_t *self, const void *const old_params,

```
....
91.      dt_imageio_gallery_t *n = (dt_imageio_gallery_t
*)malloc(sizeof(dt_imageio_gallery_t));
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=50
Status	New

The gui_init method calls the d function, at line 145 of darktable/gallery.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	darktable/gallery.c	darktable/gallery.c
Line	147	147
Object	d	d

Code Snippet
File Name darktable/gallery.c
Method void gui_init(dt_imageio_module_storage_t *self)

```
....
147.    gallery_t *d = (gallery_t *)malloc(sizeof(gallery_t));
```

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=1050079&projectid=50069&pathid=128
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	885	885
Object	DT_SIGNAL_MOUSE_OVER_IMAGE_CHANGE	DT_SIGNAL_MOUSE_OVER_IMAGE_CHANGE

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
885.          CHKSIGDBG(DT_SIGNAL_MOUSE_OVER_IMAGE_CHANGE);
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=129
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	886	886
Object	DT_SIGNAL_ACTIVE_IMAGES_CHANGE	DT_SIGNAL_ACTIVE_IMAGES_CHANGE

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
886.          CHKSIGDBG(DT_SIGNAL_ACTIVE_IMAGES_CHANGE);
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=130
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	887	887
Object	DT_SIGNAL_CONTROL_REDRAW_ALL	DT_SIGNAL_CONTROL_REDRAW_ALL

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
887.          CHKSIGDBG(DT_SIGNAL_CONTROL_REDRAW_ALL);
```

Unchecked Array Index\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=131
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	888	888
Object	DT_SIGNAL_CONTROL_REDRAW_CENTER	DT_SIGNAL_CONTROL_REDRAW_CENTER

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
888.          CHKSIGDBG(DT_SIGNAL_CONTROL_REDRAW_CENTER);
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=132
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	889	889
Object	DT_SIGNAL_VIEWMANAGER_VIEW_CHANGED	DT_SIGNAL_VIEWMANAGER_VIEW_CHANGED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
889.          CHKSIGDBG(DT_SIGNAL_VIEWMANAGER_VIEW_CHANGED);
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=133
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	890	890
Object	DT_SIGNAL_VIEWMANAGER_THUMBTABLE_ACTIVATE	DT_SIGNAL_VIEWMANAGER_THUMBTABLE_ACTIVATE

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
890.          CHKSIGDBG(DT_SIGNAL_VIEWMANAGER_THUMBTABLE_ACTIVATE);
```

Unchecked Array Index\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=134
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	891	891
Object	DT_SIGNAL_COLLECTION_CHANGED	DT_SIGNAL_COLLECTION_CHANGED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
891.          CHKSIGDBG(DT_SIGNAL_COLLECTION_CHANGED);
```

Unchecked Array Index\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=135
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	892	892

Object	DT_SIGNAL_SELECTION_CHANGED	DT_SIGNAL_SELECTION_CHANGED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
892.          CHKSIGDBG(DT_SIGNAL_SELECTION_CHANGED);
```

Unchecked Array Index\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=136
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	893	893
Object	DT_SIGNAL_TAG_CHANGED	DT_SIGNAL_TAG_CHANGED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
893.          CHKSIGDBG(DT_SIGNAL_TAG_CHANGED);
```

Unchecked Array Index\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=137
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	894	894
Object	DT_SIGNAL_METADATA_CHANGED	DT_SIGNAL_METADATA_CHANGED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
894.          CHKSIGDBG(DT_SIGNAL_METADATA_CHANGED);
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=138
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	895	895
Object	DT_SIGNAL_IMAGE_INFO_CHANGED	DT_SIGNAL_IMAGE_INFO_CHANGED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
895.          CHKSIGDBG(DT_SIGNAL_IMAGE_INFO_CHANGED);
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=139
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	896	896
Object	DT_SIGNAL_STYLE_CHANGED	DT_SIGNAL_STYLE_CHANGED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
896.          CHKSIGDBG(DT_SIGNAL_STYLE_CHANGED);
```

Unchecked Array Index\Path 13:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=140
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	897	897
Object	DT_SIGNAL_IMAGES_ORDER_CHANGE	DT_SIGNAL_IMAGES_ORDER_CHANGE

Code Snippet

File Name darktable/darktable.c

Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
897.          CHKSIGDBG(DT_SIGNAL_IMAGES_ORDER_CHANGE);
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=141
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	898	898
Object	DT_SIGNAL_FILMROLLS_CHANGED	DT_SIGNAL_FILMROLLS_CHANGED

Code Snippet

File Name darktable/darktable.c

Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
898.          CHKSIGDBG(DT_SIGNAL_FILMROLLS_CHANGED);
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=142
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	899	899
Object	DT_SIGNAL_FILMROLLS_IMPORTED	DT_SIGNAL_FILMROLLS_IMPORTED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
899.          CHKSIGDBG(DT_SIGNAL_FILMROLLS_IMPORTED);
```

Unchecked Array Index\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=143
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	900	900
Object	DT_SIGNAL_FILMROLLS_REMOVED	DT_SIGNAL_FILMROLLS_REMOVED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
900.          CHKSIGDBG(DT_SIGNAL_FILMROLLS_REMOVED);
```

Unchecked Array Index\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=144
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	901	901
Object	DT_SIGNAL_DEVELOP_INITIALIZE	DT_SIGNAL_DEVELOP_INITIALIZE

Code Snippet	
File Name	darktable/darktable.c
Method	int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
901.          CHKSIGDBG(DT_SIGNAL_DEVELOP_INITIALIZE);
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=145
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	902	902
Object	DT_SIGNAL_DEVELOP_MIPMAP_UPDATED	DT_SIGNAL_DEVELOP_MIPMAP_UPDATED

Code Snippet	
File Name	darktable/darktable.c
Method	int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
902.          CHKSIGDBG(DT_SIGNAL_DEVELOP_MIPMAP_UPDATED);
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=146
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	903	903
Object	DT_SIGNAL_DEVELOP_PREVIEW_PIPE_FINISHED	DT_SIGNAL_DEVELOP_PREVIEW_PIPE_FINISHED

Code Snippet	
File Name	darktable/darktable.c
Method	int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
903.          CHKSIGDBG(DT_SIGNAL_DEVELOP_PREVIEW_PIPE_FINISHED);
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=147
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	904	904
Object	DT_SIGNAL_DEVELOP_PREVIEW2_PIPE_FINISHED	DT_SIGNAL_DEVELOP_PREVIEW2_PIPE_FINISHED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
904.          CHKSIGDBG(DT_SIGNAL_DEVELOP_PREVIEW2_PIPE_FINISHED);
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=148
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	905	905
Object	DT_SIGNAL_DEVELOP_UI_PIPE_FINISHED	DT_SIGNAL_DEVELOP_UI_PIPE_FINISHED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
905.          CHKSIGDBG(DT_SIGNAL_DEVELOP_UI_PIPE_FINISHED);
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=149
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	906	906
Object	DT_SIGNAL_DEVELOP_HISTORY_WILL_CHANGE	DT_SIGNAL_DEVELOP_HISTORY_WILL_CHANGE

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
906.          CHKSIGDBG(DT_SIGNAL_DEVELOP_HISTORY_WILL_CHANGE);
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=150
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	907	907
Object	DT_SIGNAL_DEVELOP_HISTORY_CHANGE	DT_SIGNAL_DEVELOP_HISTORY_CHANGE

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
907.          CHKSIGDBG(DT_SIGNAL_DEVELOP_HISTORY_CHANGE);
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=500

	69&pathid=151
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	908	908
Object	DT_SIGNAL_DEVELOP_MODULE_REMOVE	DT_SIGNAL_DEVELOP_MODULE_REMOVE

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
908.          CHKSIGDBG(DT_SIGNAL_DEVELOP_MODULE_REMOVE);
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=152
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	909	909
Object	DT_SIGNAL_DEVELOP_MODULE_MOVED	DT_SIGNAL_DEVELOP_MODULE_MOVED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
909.          CHKSIGDBG(DT_SIGNAL_DEVELOP_MODULE_MOVED);
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=153
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c

Line	910	910
Object	DT_SIGNAL_DEVELOP_IMAGE_CHANGED	DT_SIGNAL_DEVELOP_IMAGE_CHANGED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
910.          CHKSIGDBG(DT_SIGNAL_DEVELOP_IMAGE_CHANGED);
```

Unchecked Array Index\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=154
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	911	911
Object	DT_SIGNAL_CONTROL_PROFILE_CHANGED	DT_SIGNAL_CONTROL_PROFILE_CHANGED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
911.          CHKSIGDBG(DT_SIGNAL_CONTROL_PROFILE_CHANGED);
```

Unchecked Array Index\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=155
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	912	912
Object	DT_SIGNAL_CONTROL_PROFILE_USER_CHANGED	DT_SIGNAL_CONTROL_PROFILE_USER_CHANGED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
912.          CHKSIGDBG(DT_SIGNAL_CONTROL_PROFILE_USER_CHANGED);
```

Unchecked Array Index\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=156
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	913	913
Object	DT_SIGNAL_IMAGE_IMPORT	DT_SIGNAL_IMAGE_IMPORT

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
913.          CHKSIGDBG(DT_SIGNAL_IMAGE_IMPORT);
```

Unchecked Array Index\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=157
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	914	914
Object	DT_SIGNAL_IMAGE_EXPORT_TMPFILE	DT_SIGNAL_IMAGE_EXPORT_TMPFILE

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
914.          CHKSIGDBG(DT_SIGNAL_IMAGE_EXPORT_TMPFILE);
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=158
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	915	915
Object	DT_SIGNAL_IMAGEIO_STORAGE_CHANGE	DT_SIGNAL_IMAGEIO_STORAGE_CHANGE

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
915.          CHKSIGDBG(DT_SIGNAL_IMAGEIO_STORAGE_CHANGE);
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=159
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	916	916
Object	DT_SIGNAL_PREFERENCES_CHANGE	DT_SIGNAL_PREFERENCES_CHANGE

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
916.          CHKSIGDBG(DT_SIGNAL_PREFERENCES_CHANGE);
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=160
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	917	917
Object	DT_SIGNAL_CAMERA_DETECTED	DT_SIGNAL_CAMERA_DETECTED

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
917.          CHKSIGDBG(DT_SIGNAL_CAMERA_DETECTED);
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=161
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	918	918
Object	DT_SIGNAL_CONTROL_NAVIGATION_REDRAW	DT_SIGNAL_CONTROL_NAVIGATION_REDRAW

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
918.          CHKSIGDBG(DT_SIGNAL_CONTROL_NAVIGATION_REDRAW);
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=162
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	919	919
Object	DT_SIGNAL_CONTROL_LOG_REDRAW	DT_SIGNAL_CONTROL_LOG_REDRAW

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
919.          CHKSIGDBG(DT_SIGNAL_CONTROL_LOG_REDRAW);
```

Unchecked Array Index\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=163
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	920	920
Object	DT_SIGNAL_CONTROL_TOAST_REDRAW	DT_SIGNAL_CONTROL_TOAST_REDRAW

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
920.          CHKSIGDBG(DT_SIGNAL_CONTROL_TOAST_REDRAW);
```

Unchecked Array Index\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=164
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	921	921

Object	DT_SIGNAL_CONTROL_PICKERDATA_READY	DT_SIGNAL_CONTROL_PICKERDATA_READY

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
921.          CHKSIGDBG(DT_SIGNAL_CONTROL_PICKERDATA_READY);
```

Unchecked Array Index\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=165
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	922	922
Object	DT_SIGNAL_METADATA_UPDATE	DT_SIGNAL_METADATA_UPDATE

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
922.          CHKSIGDBG(DT_SIGNAL_METADATA_UPDATE);
```

Unchecked Array Index\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=166
Status New

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	1019	1019
Object	n	n

Code Snippet
File Name darktable/lstrlib.c
Method static lua_Number adddigit (char *buff, int n, lua_Number x) {

```
....
1019.    buff[n] = (d < 10 ? d + '0' : d - 10 + 'a');  /* add to buffer
*/
```

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=1050079&projectid=50069&pathid=98
Status	New

The variable declared in 0 at darktable/lgc.c in line 125 is not initialized when it is used by gray at darktable/lgc.c in line 652.

	Source	Destination
File	darktable/lgc.c	darktable/lgc.c
Line	137	655
Object	0	gray

Code Snippet
File Name darktable/lgc.c
Method static GCObject **getgclist (GCObject *o) {

```
....
137.      default: lua_assert(0); return 0;
```

File Name darktable/lgc.c
Method static lu_mem propagatemark (global_State *g) {

```
....
655.    g->gray = *getgclist(o);  /* remove from 'gray' list */
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=99

Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by minQuantizer at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	465
Object	encoder	minQuantizer

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
465.    switch(d->compression_type)
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=100
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by speed at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	463
Object	encoder	speed

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
463.    }
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=101

Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by maxQuantizer at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	466
Object	encoder	maxQuantizer

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
466.    {
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=102
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by speed at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	470
Object	encoder	speed

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
470.
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=103

Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by maxQuantizer at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	472
Object	encoder	maxQuantizer

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
472.        encoder->maxQuantizer = AVIF_QUANTIZER_LOSSLESS;
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=104
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by maxQuantizer at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	473
Object	encoder	maxQuantizer

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
473.
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=105

Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by maxQuantizer at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	473
Object	encoder	maxQuantizer

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
473.
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=106
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by minQuantizer at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	475
Object	encoder	minQuantizer

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
475.      case AVIF_COMP_LOSSY:
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=107

Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by minQuantizer at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	476
Object	encoder	minQuantizer

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
476.        encoder->speed = AVIF_SPEED_DEFAULT;
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=108
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by minQuantizer at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	476
Object	encoder	minQuantizer

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
476.        encoder->speed = AVIF_SPEED_DEFAULT;
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=109

Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by tileColsLog2 at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	510
Object	encoder	tileColsLog2

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
510.            height_tile_size = AVIF_MIN_TILE_SIZE * 4;
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=110
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by tileRowsLog2 at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	511
Object	encoder	tileRowsLog2

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
511.        }
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=111

Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by tileRowsLog2 at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	517
Object	encoder	tileRowsLog2

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
517.        encoder->tileRowsLog2 = floor_log2(height /
height_tile_size) / 2;
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=112
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by tileColsLog2 at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	517
Object	encoder	tileColsLog2

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
517.        encoder->tileRowsLog2 = floor_log2(height /
height_tile_size) / 2;
```

NULL Pointer Dereference\Path 16:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=113
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by maxThreads at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	519
Object	encoder	maxThreads

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
519.        /*
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=114
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by maxQuantizer at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	529
Object	encoder	maxQuantizer

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
529.    }
```

NULL Pointer Dereference\Path 18:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=115
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by minQuantizer at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	530
Object	encoder	minQuantizer

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
530.
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=116
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by tileColsLog2 at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	531
Object	encoder	tileColsLog2

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
531.    dt_print(DT_DEBUG_IMAGEIO,
```

NULL Pointer Dereference\Path 20:

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

	BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=117
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by tileRowsLog2 at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	532
Object	encoder	tileRowsLog2

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
532.             "[avif quality: %u => maxQuantizer: %u, minQuantizer:
%u, "
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=118
Status	New

The variable declared in encoder at darktable/avif.c in line 206 is not initialized when it is used by maxThreads at darktable/avif.c in line 206.

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	224	533
Object	encoder	maxThreads

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
224.    avifEncoder *encoder = NULL;
....
533.             "tileColsLog2: %u, tileRowsLog2: %u, threads: %u]\n",
```

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=1050079&projectid=50069&pathid=268
Status	New

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	439	439
Object	fgets	fgets

Code Snippet
File Name darktable/conf.c
Method gchar *dt_conf_read_values(const char *filename,

```
....
439.        const char* ret = fgets(line, LINE_SIZE, f);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=269
Status	New

	Source	Destination
File	darktable/conf.c	darktable/conf.c
Line	439	439
Object	line	line

Code Snippet
File Name darktable/conf.c
Method gchar *dt_conf_read_values(const char *filename,

```
....
439.        const char* ret = fgets(line, LINE_SIZE, f);
```

Improper Resource Access Authorization\Path 3:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=270
Status	New

	Source	Destination
File	darktable/imageio_jpeg.c	darktable/imageio_jpeg.c
Line	761	761
Object	first3bytes	first3bytes

Code Snippet
File Name darktable/imageio_jpeg.c
Method dt_imageio_retval_t dt_imageio_open_jpeg(dt_image_t *img,

```
....
761.    if(fread(first3bytes, 1, 3, f) != 3)
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=271
Status	New

	Source	Destination
File	darktable/mipmap_cache.c	darktable/mipmap_cache.c
Line	375	375
Object	blob	blob

Code Snippet
File Name darktable/mipmap_cache.c
Method void dt_mipmap_cache_allocate_dynamic(void *data, dt_cache_entry_t *entry)

```
....
375.          const int rd = fread(blob, sizeof(uint8_t), len, f);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=272
Status	New

	Source	Destination
File	darktable/conf.c	darktable/conf.c

Line	824	824
Object	fprintf	fprintf

Code Snippet
File Name darktable/conf.c
Method static void dt_conf_print(const gchar *key, const gchar *val, FILE *f)

```
....
824.    fprintf(f, "%s=%s\n", key, val);
```

Improper Resource Access Authorization\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=273
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	466	466
Object	fprintf	fprintf

Code Snippet
File Name darktable/darktable.c
Method void dt_dump_pfm_file(

```
....
466.      fprintf(f, "P5\n%d %d\n", width, height);
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=274
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	468	468
Object	fprintf	fprintf

Code Snippet
File Name darktable/darktable.c
Method void dt_dump_pfm_file(

```
....
468.      fprintf(f, "P%s\n%d %d\n-1.0\n", (bpp != 16) ? "f" : "F",
width, height);
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=275
Status	New

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	426	426
Object	fprintf	fprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
426.    fprintf(f,
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=276
Status	New

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	449	449
Object	fprintf	fprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
449.      fprintf(f, "%s", p->line);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=277
Status	New

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	453	453
Object	fprintf	fprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
453.    fprintf(f, "        <p style=\"clear:both;\"></p>\n"
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=278
Status	New

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	506	506
Object	fprintf	fprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
506.      fprintf(f, "%s", p->item);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=279
Status	New

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	510	510
Object	fprintf	fprintf

Code Snippet
File Name darktable/gallery.c
Method void finalize_store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *dd)

```
....
510.    fprintf(f, "];\n"
```

Improper Resource Access Authorization\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=280
Status New

	Source	Destination
File	darktable/avif.c	darktable/avif.c
Line	569	569
Object	fwrite	fwrite

Code Snippet
File Name darktable/avif.c
Method int write_image(struct dt_imageio_module_data_t *data,

```
....
569.    if(f == NULL)
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=281
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	475	475
Object	fwrite	fwrite

Code Snippet
File Name darktable/darktable.c
Method void dt_dump_pfm_file(

```
....
475.        fwrite(data + blk, (bpp==16) ? 12 : bpp, 1, f);
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=53
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	721	721
Object	sizeof	sizeof

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
721.                CHAR_BIT * sizeof(void *)
```

Use of Sizeof On a Pointer Type\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=54
Status New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	1912	1912
Object	sizeof	sizeof

Code Snippet
File Name darktable/darktable.c
Method void dt_configure_runtime_performance(const int old, char *info)

```
....
1912.    const size_t bits = CHAR_BIT * sizeof(void *);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=55
Status	New

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	528	528
Object	sizeof	sizeof

Code Snippet
File Name darktable/gallery.c
Method size_t params_size(dt_imageio_module_storage_t *self)

```
....
528.    return sizeof(dt_imageio_gallery_t) - 2 * sizeof(void *) -
DT_MAX_PATH_FOR_PARAMS;
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=56
Status	New

	Source	Destination
File	darktable/lobject.c	darktable/lobject.c
Line	508	508
Object	sizeof	sizeof

Code Snippet
File Name darktable/lobject.c
Method const char *luaO_pushvfstring (lua_State *L, const char *fmt, va_list argp) {

```
....
508.          const int sz = 3 * sizeof(void*) + 8; /* enough space for
'%p' */
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low

Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=57
Status	New

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	679	679
Object	sizeof	sizeof

Code Snippet
File Name darktable/types.c
Method luaA_Type dt_lua_init_singleton(lua_State *L, const char *unique_name, void *data)

```
....
679.    luaA_Type type_id = luaA_type_add(L, tmp_name, sizeof(void *));
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=58
Status	New

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	682	682
Object	sizeof	sizeof

Code Snippet
File Name darktable/types.c
Method luaA_Type dt_lua_init_singleton(lua_State *L, const char *unique_name, void *data)

```
....
682.    void **udata = lua_newuserdatauv(L, sizeof(void *), 1);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=59
Status	New

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	687	687
Object	sizeof	sizeof

Code Snippet
File Name darktable/types.c
Method luaA_Type dt_lua_init_singleton(lua_State *L, const char *unique_name, void *data)

```
....
687.      memset(udata, 0, sizeof(void *));
```

Use of Sizeof On a Pointer Type\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=60
Status New

	Source	Destination
File	darktable/types.c	darktable/types.c
Line	968	968
Object	sizeof	sizeof

Code Snippet
File Name darktable/types.c
Method int dt_lua_init_early_types(lua_State *L)

```
....
968.    luaA_conversion_push_type(L,
luaA_type_add(L,"unknown",sizeof(void*)), unknown_pushfunc);
```

Potential Precision Problem

Query Path:
CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

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

Description

Potential Precision Problem\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=119

Status	New

The size of the buffer used by store in ".%s", at line 195 of darktable/gallery.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that store passes to ".%s", at line 195 of darktable/gallery.c, to overwrite the target buffer.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	265	265
Object	".%s"	".%s"

Code Snippet
File Name darktable/gallery.c
Method int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
265.    sprintf(c, ".%s", ext);
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=120
Status	New

The size of the buffer used by store in "-thumb.%s", at line 195 of darktable/gallery.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that store passes to "-thumb.%s", at line 195 of darktable/gallery.c, to overwrite the target buffer.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	300	300
Object	"-thumb.%s"	"-thumb.%s"

Code Snippet
File Name darktable/gallery.c
Method int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
300.    sprintf(c, "-thumb.%s", ext);
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=121
Status	New

The size of the buffer used by store in "-thumb.%s", at line 195 of darktable/gallery.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that store passes to "-thumb.%s", at line 195 of darktable/gallery.c, to overwrite the target buffer.

	Source	Destination
File	darktable/gallery.c	darktable/gallery.c
Line	365	365
Object	"-thumb.%s"	"-thumb.%s"

Code Snippet
File Name darktable/gallery.c
Method int store(dt_imageio_module_storage_t *self, dt_imageio_module_data_t *sdata, const dt_imgid_t imgid,

```
....
365.    sprintf(c, "-thumb.%s", ext);
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Arithmenic Operation On Boolean\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=126
Status New

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	157	157
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name darktable/lstrlib.c
Method static int str_rep (lua_State *L) {

```
....
157.    else if (l_unlikely(l + lsep < l || l + lsep > MAXSIZE / n))
```

Arithmenic Operation On Boolean\Path 2:

Severity Low
Result State To Verify

Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=127
Status	New

	Source	Destination
File	darktable/lstrlib.c	darktable/lstrlib.c
Line	1654	1654
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name darktable/lstrlib.c
Method static int str_packsize (lua_State *L) {

```
....
1654.      luaL_argcheck(L, totalsize <= MAXSIZE - size, 1,
```

Unreleased Resource Leak

Query Path:
CPP\Cx\CPP Low Visibility\Unreleased Resource Leak Version:0

Categories

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

Description

Unreleased Resource Leak\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050079&projectid=50069&pathid=93
Status	New

	Source	Destination
File	darktable/darktable.c	darktable/darktable.c
Line	560	560
Object	recursive_locking	recursive_locking

Code Snippet
File Name darktable/darktable.c
Method int dt_init(int argc, char *argv[], const gboolean init_gui, const gboolean load_data, lua_State *L)

```
....
560.    pthread_mutexattr_init(&recursive_locking);
```

Buffer Overflow IndexFromInput

Risk

What might happen

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

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

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

Source Code Examples

Buffer Overflow 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));
    }
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

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

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;
}
```

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;
}
```

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 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());
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Resource Locking Problems

Category ID: 411 *(Category)* **Status:** Draft

Description

Description Summary

Weaknesses in this category are related to improper handling of locks that are used to control access to resources.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	412	Unrestricted Externally Accessible Lock	Development Concepts699
ParentOf	Weakness Base	413	Insufficient Resource Locking	**Development Concepts (primary)699**
ParentOf	Weakness Base	414	Missing Lock Check	**Development Concepts (primary)699**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Resource Locking problems

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		

BACK TO TOP

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

Potential Precision Problem

Risk

What might happen

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

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

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

Source Code Examples

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Code Quality		

BACK TO TOP

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

Scanned Languages

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