

## reading-code-of-nginx-1.9.2 Scan Report

Project Name	reading-code-of-nginx-1.9.2
Scan Start	Saturday, June 22, 2024 12:07:43 AM
Preset	Checkmarx Default
Scan Time	00h:14m:16s
Lines Of Code Scanned	68977
Files Scanned	35
Report Creation Time	Saturday, June 22, 2024 12:23:48 AM
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078</a>
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	2/1000 (Vulnerabilities/LOC)
Visibility	Public

### Filter Settings

#### **Severity**

Included: High, Medium, Low, Information

Excluded: None

#### **Result State**

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

Excluded: None

#### **Assigned to**

Included: All

#### **Categories**

Included:

Uncategorized All

Custom All

PCI DSS v3.2 All

OWASP Top 10 2013 All

FISMA 2014 All

NIST SP 800-53 All

OWASP Top 10 2017 All

OWASP Mobile Top 10  
2016 All

Excluded:

Uncategorized None

Custom None

PCI DSS v3.2 None

OWASP Top 10 2013 None

FISMA 2014 None

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

**Results Limit**

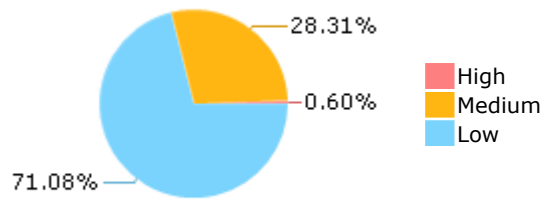
Results limit per query was set to 50

**Selected Queries**

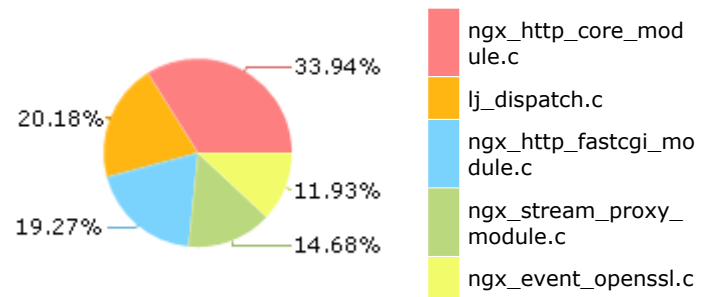
Selected queries are listed in [Result Summary](#)

---

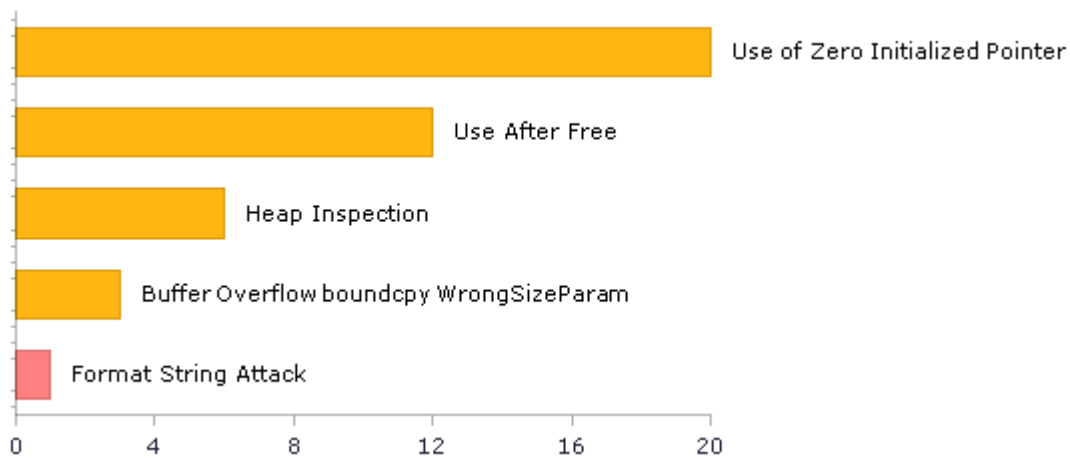
## Result Summary



## Most Vulnerable Files



## Top 5 Vulnerabilities



## Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	64	29
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	6	6
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	3	3
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	6	6
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	3	3
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

## Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	3	3
PCI DSS (3.2) - 6.5.2 - Buffer overflows	6	6
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

## Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	0	0
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	13	13
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.	6	6
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	0	0

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

## Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	0	0
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	13	13
SC-4 Information in Shared Resources (P1)	6	6
SC-5 Denial of Service Protection (P1)*	78	34
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	27	27
SI-11 Error Handling (P2)*	2	2
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	3	3

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



## Scan Summary - OWASP Mobile Top 10 2016

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

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

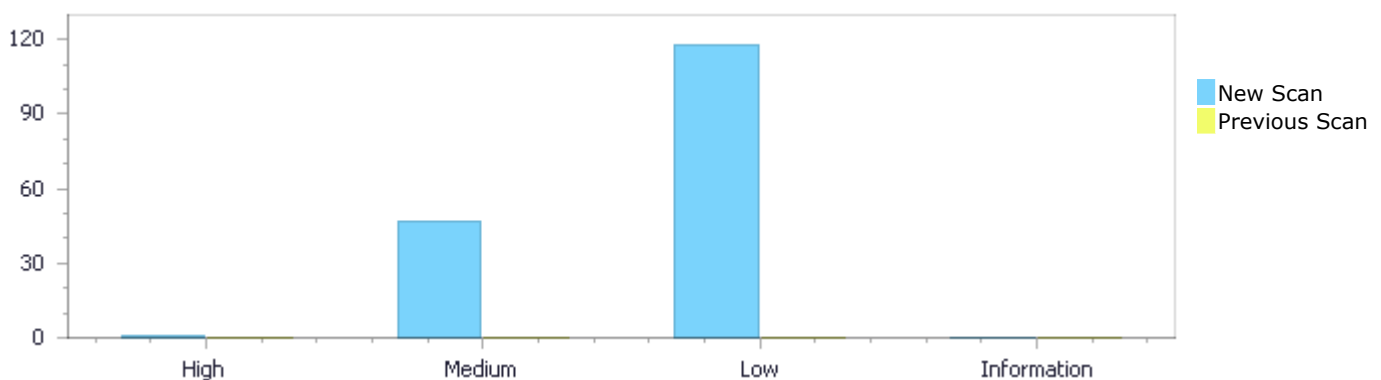
## Scan Summary - Custom

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

## Results Distribution By Status First scan of the project

	High	Medium	Low	Information	Total
New Issues	1	47	118	0	166
Recurrent Issues	0	0	0	0	0
Total	1	47	118	0	166

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	47	118	0	166
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	1	47	118	0	166

## Result Summary

Vulnerability Type	Occurrences	Severity
<a href="#">Format String Attack</a>	1	High
<a href="#">Use of Zero Initialized Pointer</a>	20	Medium
<a href="#">Use After Free</a>	12	Medium
<a href="#">Heap Inspection</a>	6	Medium
<a href="#">Buffer Overflow boundcpy WrongSizeParam</a>	3	Medium

<a href="#">Dangerous Functions</a>	3	Medium
<a href="#">Buffer Overflow AddressOfLocalVarReturned</a>	2	Medium
<a href="#">Memory Leak</a>	1	Medium
<a href="#">NULL Pointer Dereference</a>	43	Low
<a href="#">Use of Sizeof On a Pointer Type</a>	31	Low
<a href="#">Unchecked Array Index</a>	26	Low
<a href="#">Information Exposure Through Comments</a>	13	Low
<a href="#">Potential Off by One Error in Loops</a>	3	Low
<a href="#">Unchecked Return Value</a>	2	Low

## 10 Most Vulnerable Files

### High and Medium Vulnerabilities

File Name	Issues Found
reading-code-of-nginx-1.9.2/nginx_http_core_module.c	13
reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	12
reading-code-of-nginx-1.9.2/nginx_event_openssl.c	6
reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c	5
reading-code-of-nginx-1.9.2/lj_dispatch.c	4
reading-code-of-nginx-1.9.2/lj_gc.c	2
reading-code-of-nginx-1.9.2/nginx_string.c	2
reading-code-of-nginx-1.9.2/nginx_http_spdy.c	2
reading-code-of-nginx-1.9.2/nginx_resolver.c	1
reading-code-of-nginx-1.9.2/nginx_http_proxy_module.c	1

## Scan Results Details

### Format String Attack

Query Path:

CPP\Cx\CPP Buffer Overflow\Format String Attack Version:1

#### Categories

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

#### Description

##### Format String Attack\Path 1:

Severity	High
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=1">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=1</a>
Status	New

Method ngx\_udp\_connect at line 3044 of reading-code-of-nginx-1.9.2/nginx\_resolver.c receives the "<%25s, %5d> epoll read add" value from user input. This value is then used to construct a "format string" "<%25s, %5d> epoll read add", which is provided as an argument to a string formatting function in ngx\_udp\_connect method of reading-code-of-nginx-1.9.2/nginx\_resolver.c at line 3044.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_resolver.c	reading-code-of-nginx-1.9.2/nginx_resolver.c
Line	3115	3115
Object	"<%25s, %5d> epoll read add"	"<%25s, %5d> epoll read add"

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_resolver.c  
Method ngx\_udp\_connect(ngx\_udp\_connection\_t \*uc)

```
....
3115.      snprintf(tmpbuf, sizeof(tmpbuf), "<%25s, %5d> epoll
NGX_READ_EVENT(et) read add", NGX_FUNC_LINE);
```

### 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	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=1">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=1</a>

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=32](http://BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=32)

Status New

The variable declared in `body_str` at `reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c` in line 201 is not initialized when it is used by `to_write` at `reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c` in line 201.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c
Line	207	260
Object	body_str	to_write

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c

Method ngx\_http\_echo\_parse\_subrequest\_spec(ngx\_http\_request\_t \*r,

```
....
207.     ngx_str_t                *body_str = NULL;
....
260.                to_write = &body_str;
```

#### Use of Zero Initialized Pointer\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=33>

Status New

The variable declared in `body_file` at `reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c` in line 201 is not initialized when it is used by `to_write` at `reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c` in line 201.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c
Line	208	267
Object	body_file	to_write

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c

Method ngx\_http\_echo\_parse\_subrequest\_spec(ngx\_http\_request\_t \*r,

```
....
208.     ngx_str_t                *body_file = NULL;
....
267.                to_write = &body_file;
```

### Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=34">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=34</a>
Status	New

The variable declared in rb at reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c in line 201 is not initialized when it is used by rb at reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c in line 201.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c
Line	211	280
Object	rb	rb

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c  
Method ngx\_http\_echo\_parse\_subrequest\_spec(ngx\_http\_request\_t \*r,

```
....  
211.     ngx_http_request_body_t     *rb = NULL;  
....  
280.     rb = ngx_palloc(r->pool,  
sizeof(ngx_http_request_body_t));
```

### Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=35">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=35</a>
Status	New

The variable declared in rb at reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c in line 201 is not initialized when it is used by rb at reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c in line 201.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c
Line	211	324
Object	rb	rb

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c  
Method ngx\_http\_echo\_parse\_subrequest\_spec(ngx\_http\_request\_t \*r,



```
....
211.         ngx_http_request_body_t      *rb = NULL;
....
324.         rb = ngx_palloc(r->pool,
sizeof(ngx_http_request_body_t));
```

#### Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=36">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=36</a>
Status	New

The variable declared in name at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395 is not initialized when it is used by content\_handler at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2734.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2421	2811
Object	name	content_handler

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_try\_files\_phase(ngx\_http\_request\_t \*r,

```
....
2421.         name = NULL;
```



File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_update\_location\_config(ngx\_http\_request\_t \*r)

```
....
2811.         r->content_handler = clcf->handler;
```

#### Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=37">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=37</a>
Status	New

The variable declared in data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395 is not initialized when it is used by content\_handler at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2734.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2423	2811
Object	data	content_handler

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_try\_files\_phase(ngx\_http\_request\_t \*r,

```
....
2423.         path.data = NULL;
```

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_update\_location\_config(ngx\_http\_request\_t \*r)

```
....
2811.         r->content_handler = clcf->handler;
```

#### Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=38">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=38</a>
Status	New

The variable declared in cache at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 4102 is not initialized when it is used by content\_handler at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2734.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	4142	2811
Object	cache	content_handler

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_internal\_redirect(ngx\_http\_request\_t \*r,

```
....
4142.         r->cache = NULL;
```

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c

Method ngx\_http\_update\_location\_config(ngx\_http\_request\_t \*r)

```
....
2811.          r->content_handler = clcf->handler;
```

### Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=39">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=39</a>
Status	New

The variable declared in content\_handler at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 4157 is not initialized when it is used by content\_handler at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2734.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	4203	2811
Object	content_handler	content_handler

### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_named\_location(ngx\_http\_request\_t \*r, ngx\_str\_t \*name)

```
....
4203.          r->content_handler = NULL;
```



File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_update\_location\_config(ngx\_http\_request\_t \*r)

```
....
2811.          r->content_handler = clcf->handler;
```

### Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=40">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=40</a>
Status	New

The variable declared in name at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395 is not initialized when it is used by data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395.

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

File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2421	2582
Object	name	data

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_try\_files\_phase(ngx\_http\_request\_t \*r,

```
....  
2421.         name = NULL;  
....  
2582.         path.data += root;
```

#### Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=41">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=41</a>
Status	New

The variable declared in data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395 is not initialized when it is used by data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2423	2582
Object	data	data

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_try\_files\_phase(ngx\_http\_request\_t \*r,

```
....  
2423.         path.data = NULL;  
....  
2582.         path.data += root;
```

#### Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=42">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=42</a>
Status	New

The variable declared in data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395 is not initialized when it is used by data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2423	2533
Object	data	data

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_try\_files\_phase(ngx\_http\_request\_t \*r,

```
....
2423.         path.data = NULL;
....
2533.         path.data += root;
```

#### Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=43">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=43</a>
Status	New

The variable declared in data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395 is not initialized when it is used by data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2423	2478
Object	data	data

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_try\_files\_phase(ngx\_http\_request\_t \*r,

```
....
2423.         path.data = NULL;
....
2478.         path.len = (name + tf->name.len - 1) - path.data;
```

#### Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=44">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=44</a>
Status	New

The variable declared in data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395 is not initialized when it is used by data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2423	2490
Object	data	data

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_try\_files\_phase(ngx\_http\_request\_t \*r,

```
....  
2423.         path.data = NULL;  
....  
2490.         path.len = e.pos - path.data;
```

#### Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=45">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=45</a>
Status	New

The variable declared in data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395 is not initialized when it is used by data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2423	2469
Object	data	data

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_try\_files\_phase(ngx\_http\_request\_t \*r,

```
....  
2423.         path.data = NULL;  
....  
2469.         name = path.data + root;
```

#### Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=46">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=46</a>

Status New

The variable declared in data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 2395 is not initialized when it is used by data at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 3426.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2423	3481
Object	data	data

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_try\_files\_phase(ngx\_http\_request\_t \*r,

```
....
2423.         path.data = NULL;
```

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_map\_uri\_to\_path(ngx\_http\_request\_t \*r, ngx\_str\_t \*path,

```
....
3481.         last = path->data + *root_length;
```

#### Use of Zero Initialized Pointer\Path 16:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=47>  
Status New

The variable declared in out at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 3927 is not initialized when it is used by next at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 3927.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	4065	4072
Object	out	next

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_subrequest(ngx\_http\_request\_t \*r,

```
....  
4065.      pr->out = NULL;  
....  
4072.      p->next = pr;
```

#### Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=48">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=48</a>
Status	New

The variable declared in next at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 3927 is not initialized when it is used by next at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 3927.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	4066	4072
Object	next	next

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_subrequest(ngx\_http\_request\_t \*r,

```
....  
4066.      pr->next = NULL;  
....  
4072.      p->next = pr;
```

#### Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=49">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=49</a>
Status	New

The variable declared in BinaryExpr at reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c in line 201 is not initialized when it is used by to\_write at reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c in line 201.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c
Line	205	244
Object	BinaryExpr	to_write



**Code Snippet**

File Name reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c  
Method ngx\_http\_echo\_parse\_subrequest\_spec(ngx\_http\_request\_t \*r,

```
....  
205.         ngx_str_t                 **to_write = NULL;  
....  
244.         *to_write = arg;
```

**Use of Zero Initialized Pointer\Path 19:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=50>  
Status New

The variable declared in out at reading-code-of-nginx-1.9.2/nginx\_http\_proxy\_module.c in line 2233 is not initialized when it is used by next at reading-code-of-nginx-1.9.2/nginx\_http\_proxy\_module.c in line 2233.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_http_proxy_module.c
Line	2254	2341
Object	out	next

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/nginx\_http\_proxy\_module.c  
Method ngx\_http\_proxy\_body\_output\_filter(void \*data, ngx\_chain\_t \*in)

```
....  
2254.         out = NULL;  
....  
2341.         tl->next = *fl;
```

**Use of Zero Initialized Pointer\Path 20:**

Severity Medium  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=51>  
Status New

The variable declared in frame at reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c in line 663 is not initialized when it is used by last\_out at reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c in line 663.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_spdy.c	reading-code-of-nginx-1.9.2/nginx_http_spdy.c
Line	776	784

Object	frame	last_out
--------	-------	----------

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c

Method ngx\_http\_spdy\_send\_output\_queue(ngx\_http\_spdy\_connection\_t \*sc)

```
....
776.         frame = NULL;
....
784.         sc->last_out = frame;
```

## Use After Free

Query Path:

CPP\Cx\CPP Medium Threat\Use After Free Version:1

### Categories

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

OWASP Top 10 2017: A1-Injection

### Description

#### Use After Free\Path 1:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=20>

Status New

The pointer connection at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1089 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1102	1118
Object	Address	connection

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c

Method ngx\_stream\_proxy\_next\_upstream(ngx\_stream\_session\_t \*s)

```
....
1102.         u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);
....
1118.         pc = u->peer.connection;
```

#### Use After Free\Path 2:

Severity Medium

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=20>

Status	<a href="#">78&amp;pathid=21</a> New
--------	---

The pointer peer at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1089 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1102	1118
Object	Address	peer

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_next\_upstream(ngx\_stream\_session\_t \*s)

```
....  
1102.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);  
....  
1118.          pc = u->peer.connection;
```

#### Use After Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=22">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=22</a>
Status	New

The pointer peer at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1089 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1102	1118
Object	data	peer

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_next\_upstream(ngx\_stream\_session\_t \*s)

```
....  
1102.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);  
....  
1118.          pc = u->peer.connection;
```

#### Use After Free\Path 4:

Severity	Medium
Result State	To Verify

Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=23">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=23</a>
Status	New

The pointer tries at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1089 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1102	1110
Object	Address	tries

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_next\_upstream(ngx\_stream\_session\_t \*s)

```
....  
1102.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);  
....  
1110.          if (u->peer.tries == 0
```

#### Use After Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=24">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=24</a>
Status	New

The pointer peer at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1089 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1102	1110
Object	Address	peer

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_next\_upstream(ngx\_stream\_session\_t \*s)

```
....  
1102.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);  
....  
1110.          if (u->peer.tries == 0
```

#### Use After Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=25">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=25</a>
Status	New

The pointer peer at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1089 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1102	1110
Object	data	peer

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_next\_upstream(ngx\_stream\_session\_t \*s)

```
....  
1102.         u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);  
....  
1110.         if (u->peer.tries == 0
```

#### Use After Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=26">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=26</a>
Status	New

The pointer start\_time at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1089 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1102	1112
Object	Address	start_time

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_next\_upstream(ngx\_stream\_session\_t \*s)

```
.....
1102.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);
.....
1112.          || (timeout && ngx_current_msec - u->peer.start_time >=
timeout))
```

#### Use After Free\Path 8:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=27">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=27</a>
Status	New

The pointer peer at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1089 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1102	1112
Object	Address	peer

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_next\_upstream(ngx\_stream\_session\_t \*s)

```
.....
1102.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);
.....
1112.          || (timeout && ngx_current_msec - u->peer.start_time >=
timeout))
```

#### Use After Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=28">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=28</a>
Status	New

The pointer peer at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1089 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1102	1112
Object	data	peer

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_next\_upstream(ngx\_stream\_session\_t \*s)

```
....
1102.          u->peer.free(&u->peer, u->peer.data, NGX_PEER_FAILED);
....
1112.          || (timeout && ngx_current_msec - u->peer.start_time >=
timeout))
```

#### Use After Free\Path 10:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=29>  
Status New

The pointer connection at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1142 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1157	1161
Object	Address	connection

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_finalize(ngx\_stream\_session\_t \*s, ngx\_int\_t rc)

```
....
1157.          u->peer.free(&u->peer, u->peer.data, 0);
....
1161.          pc = u->peer.connection;
```

#### Use After Free\Path 11:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=30>  
Status New

The pointer peer at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1142 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c

Line	1157	1161
Object	Address	peer

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_finalize(ngx\_stream\_session\_t \*s, ngx\_int\_t rc)

```
....
1157.         u->peer.free(&u->peer, u->peer.data, 0);
....
1161.         pc = u->peer.connection;
```

#### Use After Free\Path 12:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=31>  
Status New

The pointer peer at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 1142 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	1157	1161
Object	data	peer

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_finalize(ngx\_stream\_session\_t \*s, ngx\_int\_t rc)

```
....
1157.         u->peer.free(&u->peer, u->peer.data, 0);
....
1161.         pc = u->peer.connection;
```

## Heap Inspection

Query Path:

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

### Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure  
FISMA 2014: Media Protection  
NIST SP 800-53: SC-4 Information in Shared Resources (P1)  
OWASP Top 10 2017: A3-Sensitive Data Exposure

### Description

#### Heap Inspection\Path 1:

Severity Medium



Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=13">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=13</a>
Status	New

Method ngx\_ssl\_read\_password\_file at line 763 of reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c defines passwords, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwords, this variable is never cleared from memory.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	770	770
Object	passwords	passwords

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
Method ngx\_ssl\_read\_password\_file(ngx\_conf\_t \*cf, ngx\_str\_t \*file)

```
....
770.     ngx_array_t     *passwords;
```

### Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=14">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=14</a>
Status	New

Method ngx\_ssl\_passwords\_cleanup at line 889 of reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c defines passwords, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwords, this variable is never cleared from memory.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	891	891
Object	passwords	passwords

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
Method ngx\_ssl\_passwords\_cleanup(void \*data)

```
....
891.     ngx_array_t *passwords = data;
```

### Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify

Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=15">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=15</a>
Status	New

Method ngx\_ssl\_certificate at line 301 of reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	307	307
Object	pwd	pwd

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
Method ngx\_ssl\_certificate(ngx\_conf\_t \*cf, ngx\_ssl\_t \*ssl, ngx\_str\_t \*cert,

```
....
307.     ngx_str_t     *pwd;
```

#### Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=16">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=16</a>
Status	New

Method ngx\_ssl\_read\_password\_file at line 763 of reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	769	769
Object	pwd	pwd

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
Method ngx\_ssl\_read\_password\_file(ngx\_conf\_t \*cf, ngx\_str\_t \*file)

```
....
769.     ngx_str_t     *pwd;
```

#### Heap Inspection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=16">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=16</a>

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=17](http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=17)

Status New

Method ngx\_ssl\_passwords\_cleanup at line 889 of reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	893	893
Object	pwd	pwd

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
Method ngx\_ssl\_passwords\_cleanup(void \*data)

```
....
893.     ngx_str_t    *pwd;
```

### Heap Inspection\Path 6:

Severity Medium  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=18>  
Status New

Method ngx\_ssl\_password\_callback at line 497 of reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	499	499
Object	pwd	pwd

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
Method ngx\_ssl\_password\_callback(char \*buf, int size, int rwflag, void \*userdata)

```
....
499.     ngx_str_t *pwd = userdata;
```

## 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	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=7">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=7</a>
Status	New

The size of the buffer used by `lj_dispatch_update` in `GG_LEN_SDISP`, at line 92 of `reading-code-of-nginx-1.9.2/lj_dispatch.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `lj_dispatch_update` passes to `GG_LEN_SDISP`, at line 92 of `reading-code-of-nginx-1.9.2/lj_dispatch.c`, to overwrite the target buffer.

	Source	Destination
File	<code>reading-code-of-nginx-1.9.2/lj_dispatch.c</code>	<code>reading-code-of-nginx-1.9.2/lj_dispatch.c</code>
Line	133	133
Object	<code>GG_LEN_SDISP</code>	<code>GG_LEN_SDISP</code>

#### Code Snippet

File Name `reading-code-of-nginx-1.9.2/lj_dispatch.c`  
Method `void lj_dispatch_update(global_State *g)`

```
....
133.      memcpy(&disp[0], &disp[GG_LEN_DDISP],
GG_LEN_SDISP*sizeof(ASMFunction));
```

#### **Buffer Overflow boundcpy WrongSizeParam\Path 2:**

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=8">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=8</a>
Status	New

The size of the buffer used by `lj_dispatch_update` in `ASMFunction`, at line 92 of `reading-code-of-nginx-1.9.2/lj_dispatch.c`, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that `lj_dispatch_update` passes to `ASMFunction`, at line 92 of `reading-code-of-nginx-1.9.2/lj_dispatch.c`, to overwrite the target buffer.

	Source	Destination
File	<code>reading-code-of-nginx-1.9.2/lj_dispatch.c</code>	<code>reading-code-of-nginx-1.9.2/lj_dispatch.c</code>
Line	133	133
Object	<code>ASMFunction</code>	<code>ASMFunction</code>

#### Code Snippet

File Name `reading-code-of-nginx-1.9.2/lj_dispatch.c`

Method void lj\_dispatch\_update(global\_State \*g)

```
....
133.         memcpy(&disp[0], &disp[GG_LEN_DDISP],
GG_LEN_SDISP*sizeof(ASMFunction));
```

### Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=9">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=9</a>
Status	New

The size of the buffer used by ngx\_memcpy in n, at line 2228 of reading-code-of-nginx-1.9.2/nginx\_string.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ngx\_memcpy passes to n, at line 2228 of reading-code-of-nginx-1.9.2/nginx\_string.c, to overwrite the target buffer.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_string.c	reading-code-of-nginx-1.9.2/nginx_string.c
Line	2235	2235
Object	n	n

### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_string.c  
Method ngx\_memcpy(void \*dst, const void \*src, size\_t n)

```
....
2235.         return memcpy(dst, src, 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	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=10">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=10</a>
Status	New

The dangerous function, memcpy, was found in use at line 49 in reading-code-of-nginx-1.9.2/lj\_dispatch.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	67	67
Object	memcpy	memcpy

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_init(GG\_State \*GG)

```
....  
67.     memcpy(GG->got, dispatch_got, LJ_GOT__MAX*4);
```

#### Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=11">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=11</a>
Status	New

The dangerous function, memcpy, was found in use at line 92 in reading-code-of-nginx-1.9.2/lj\_dispatch.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	133	133
Object	memcpy	memcpy

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
....  
133.     memcpy(&disp[0], &disp[GG_LEN_DDISP],  
GG_LEN_SDISP*sizeof(ASMFunction));
```

#### Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=12">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=12</a>
Status	New

The dangerous function, memcpy, was found in use at line 2228 in reading-code-of-nginx-1.9.2/nginx\_string.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_string.c	reading-code-of-nginx-1.9.2/nginx_string.c
Line	2235	2235
Object	memcpy	memcpy

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_string.c  
Method ngx\_memcpy(void \*dst, const void \*src, size\_t n)

```
....
2235.     return memcpy(dst, src, n);
```

## Buffer Overflow AddressOfLocalVarReturned

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow AddressOfLocalVarReturned Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows  
NIST SP 800-53: SC-5 Denial of Service Protection (P1)  
OWASP Top 10 2017: A1-Injection

### Description

#### Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=5">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=5</a>
Status	New

The pointer top at reading-code-of-nginx-1.9.2/lj\_gc.c in line 266 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_gc.c	reading-code-of-nginx-1.9.2/lj_gc.c
Line	279	279
Object	top	top

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_gc.c  
Method static MSize gc\_traverse\_frames(global\_State \*g, lua\_State \*th)

```
....
279.     return (MSize)(top - bot); /* Return minimum needed stack size.
*/
```

#### Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify

Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=6">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=6</a>
Status	New

The pointer bot at reading-code-of-nginx-1.9.2/lj\_gc.c in line 266 is being used after it has been freed.

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_gc.c	reading-code-of-nginx-1.9.2/lj_gc.c
Line	279	279
Object	bot	bot

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_gc.c

Method static MSize gc\_traverse\_frames(global\_State \*g, lua\_State \*th)

```
....
279.     return (MSize)(top - bot);  /* Return minimum needed stack 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	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=19">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=19</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_spdy.c	reading-code-of-nginx-1.9.2/nginx_http_spdy.c
Line	2681	2681
Object	neW	neW

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c

Method ngx\_http\_spdy\_alloc\_large\_header\_buffer(ngx\_http\_request\_t \*r)

```
....
2681.     u_char                *old, *new, *p;
```



## 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	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=98">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=98</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763 is not initialized when it is used by passwords at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	804	865
Object	null	passwords

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
Method ngx\_ssl\_read\_password\_file(ngx\_conf\_t \*cf, ngx\_str\_t \*file)

```

....
804.             passwords = NULL;
....
865.     if (passwords->nelts == 0) {

```

#### NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=99">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=99</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763 is not initialized when it is used by passwords at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	832	865
Object	null	passwords

**Code Snippet****File Name** reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c**Method** ngx\_ssl\_read\_password\_file(ngx\_conf\_t \*cf, ngx\_str\_t \*file)

```
....  
832.                passwords = NULL;  
....  
865.        if (passwords->nelts == 0) {
```

**NULL Pointer Dereference\Path 3:****Severity** Low**Result State** To Verify**Online Results** <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=100>**Status** New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763 is not initialized when it is used by passwords at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	841	865
Object	null	passwords

**Code Snippet****File Name** reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c**Method** ngx\_ssl\_read\_password\_file(ngx\_conf\_t \*cf, ngx\_str\_t \*file)

```
....  
841.                passwords = NULL;  
....  
865.        if (passwords->nelts == 0) {
```

**NULL Pointer Dereference\Path 4:****Severity** Low**Result State** To Verify**Online Results** <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=101>**Status** New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763 is not initialized when it is used by passwords at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c

Line	856	865
Object	null	passwords

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
Method ngx\_ssl\_read\_password\_file(ngx\_conf\_t \*cf, ngx\_str\_t \*file)

```
....
856.             passwords = NULL;
....
865.             if (passwords->nelts == 0) {
```

#### NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=102">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=102</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763 is not initialized when it is used by passwords at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	832	840
Object	null	passwords

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
Method ngx\_ssl\_read\_password\_file(ngx\_conf\_t \*cf, ngx\_str\_t \*file)

```
....
832.             passwords = NULL;
....
840.             passwords->nelts--;
```

#### NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=103">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=103</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763 is not initialized when it is used by passwords at reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c in line 763.

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

File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	841	840
Object	null	passwords

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
Method ngx\_ssl\_read\_password\_file(ngx\_conf\_t \*cf, ngx\_str\_t \*file)

```
....
841.                                passwords = NULL;
....
840.                                passwords->nelts--;
```

#### NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=104">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=104</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c in line 201 is not initialized when it is used by file at reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c in line 201.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c
Line	208	377
Object	null	file

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c  
Method ngx\_http\_echo\_parse\_subrequest\_spec(ngx\_http\_request\_t \*r,

```
....
208.     ngx_str_t                                *body_file = NULL;
....
377.     b->file->name = *body_file;
```

#### NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=105">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=105</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816 is not initialized when it is used by buf at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	1840	2075
Object	null	buf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_body\_output\_filter(void \*data, ngx\_chain\_t \*in)

```
....  
1840.         out = NULL;  
....  
2075.                                     cl->buf->file_last - cl->buf->file_pos);
```

#### NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=106">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=106</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816 is not initialized when it is used by buf at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	1840	2075
Object	null	buf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_body\_output\_filter(void \*data, ngx\_chain\_t \*in)

```
....  
1840.         out = NULL;  
....  
2075.                                     cl->buf->file_last - cl->buf->file_pos);
```

#### NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=107">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=107</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816 is not initialized when it is used by buf at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	1840	2074
Object	null	buf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_body\_output\_filter(void \*data, ngx\_chain\_t \*in)

```
....  
1840.         out = NULL;  
....  
2074.                                cl->buf->file_pos,
```

#### NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=108">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=108</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816 is not initialized when it is used by buf at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	1840	2073
Object	null	buf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_body\_output\_filter(void \*data, ngx\_chain\_t \*in)

```
....  
1840.         out = NULL;  
....  
2073.                                cl->buf->last - cl->buf->pos,
```

#### NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=109">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=109</a>

Status New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816 is not initialized when it is used by buf at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	1840	2073
Object	null	buf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_body\_output\_filter(void \*data, ngx\_chain\_t \*in)

```
....
1840.         out = NULL;
....
2073.                                cl->buf->last - cl->buf->pos,
```

### NULL Pointer Dereference\Path 13:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=110>  
Status New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816 is not initialized when it is used by buf at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	1840	2072
Object	null	buf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_body\_output\_filter(void \*data, ngx\_chain\_t \*in)

```
....
1840.         out = NULL;
....
2072.                                cl->buf->start, cl->buf->pos,
```

### NULL Pointer Dereference\Path 14:

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

[BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=111](http://BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=111)

Status New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816 is not initialized when it is used by buf at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	1840	2072
Object	null	buf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_body\_output\_filter(void \*data, ngx\_chain\_t \*in)

```
....
1840.         out = NULL;
....
2072.         cl->buf->start, cl->buf->pos,
```

### NULL Pointer Dereference\Path 15:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=112>

Status New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816 is not initialized when it is used by buf at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	1840	2071
Object	null	buf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_body\_output\_filter(void \*data, ngx\_chain\_t \*in)

```
....
1840.         out = NULL;
....
2071.         cl->buf->in_file,
```

### NULL Pointer Dereference\Path 16:

Severity Low



Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=113">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=113</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816 is not initialized when it is used by buf at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1816.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	1840	2070
Object	null	buf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_body\_output\_filter(void \*data, ngx\_chain\_t \*in)

```
....  
1840.         out = NULL;  
....  
2070.                                cl->buf->last_buf,
```

#### NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=114">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=114</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	3751	3860
Object	null	key

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_fastcgi\_loc\_conf\_t \*conf,

```
....  
3751.         src = NULL;  
....  
3860.         ngx_memcpy(p, src[i].key.data, src[i].key.len);
```

**NULL Pointer Dereference\Path 18:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=115">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=115</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	3751	3860
Object	null	key

**Code Snippet**

File Name	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Method	ngx_http_fastcgi_init_params(ngx_conf_t *cf, ngx_http_fastcgi_loc_conf_t *conf,

```
....  
3751.         src = NULL;  
....  
3860.         ngx_memcpy(p, src[i].key.data, src[i].key.len);
```

**NULL Pointer Dereference\Path 19:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=116">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=116</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	3751	3857
Object	null	key

**Code Snippet**

File Name	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Method	ngx_http_fastcgi_init_params(ngx_conf_t *cf, ngx_http_fastcgi_loc_conf_t *conf,

```

.....
3751.          src = NULL;
.....
3857.          copy->len = src[i].key.len;

```

### NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=117">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=117</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	3751	3832
Object	null	key

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_fastcgi\_loc\_conf\_t \*conf,

```

.....
3751.          src = NULL;
.....
3832.          copy->len = src[i].key.len;

```

### NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=118">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=118</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706 is not initialized when it is used by value at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	3751	3819
Object	null	value

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_fastcgi\_loc\_conf\_t \*conf,

```
....  
3751.          src = NULL;  
....  
3819.          if (src[i].value.len == 0) {
```

#### NULL Pointer Dereference\Path 22:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=119>  
Status New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	3751	3806
Object	null	key

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_fastcgi\_loc\_conf\_t \*conf,

```
....  
3751.          src = NULL;  
....  
3806.          if (src[i].key.len > sizeof("HTTP_") - 1
```

#### NULL Pointer Dereference\Path 23:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=120>  
Status New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 3706.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	3751	3807
Object	null	key

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_fastcgi\_loc\_conf\_t \*conf,

```
....
3751.         src = NULL;
....
3807.         && ngx_strncmp(src[i].key.data, "HTTP_",
sizeof("HTTP_") - 1) == 0)
```

#### NULL Pointer Dereference\Path 24:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=121>  
Status New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c in line 663 is not initialized when it is used by stream at reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c in line 663.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_spdy.c	reading-code-of-nginx-1.9.2/nginx_http_spdy.c
Line	685	772
Object	null	stream

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c  
Method ngx\_http\_spdy\_send\_output\_queue(ngx\_http\_spdy\_connection\_t \*sc)

```
....
685.         out = NULL;
....
772.         out, out->stream ? out->stream->id : 0,
```

#### NULL Pointer Dereference\Path 25:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=122>  
Status New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c

Line	1871	1976
Object	null	key

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c  
Method ngx\_http\_uwsgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_uwsgi\_loc\_conf\_t \*conf,

```
....
1871.         src = NULL;
....
1976.         ngx_memcpy(p, src[i].key.data, src[i].key.len);
```

#### NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=123">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=123</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c
Line	1871	1976
Object	null	key

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c  
Method ngx\_http\_uwsgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_uwsgi\_loc\_conf\_t \*conf,

```
....
1871.         src = NULL;
....
1976.         ngx_memcpy(p, src[i].key.data, src[i].key.len);
```

#### NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=124">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=124</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826.

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

File	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c
Line	1871	1973
Object	null	key

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c  
Method ngx\_http\_uwsgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_uwsgi\_loc\_conf\_t \*conf,

```
....  
1871.          src = NULL;  
....  
1973.          copy->len = src[i].key.len;
```

#### NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=125">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=125</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c
Line	1871	1951
Object	null	key

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c  
Method ngx\_http\_uwsgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_uwsgi\_loc\_conf\_t \*conf,

```
....  
1871.          src = NULL;  
....  
1951.          copy->len = src[i].key.len;
```

#### NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=126">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=126</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826 is not initialized when it is used by value at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c
Line	1871	1939
Object	null	value

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c  
Method ngx\_http\_uwsgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_uwsgi\_loc\_conf\_t \*conf,

```
....  
1871.         src = NULL;  
....  
1939.         if (src[i].value.len == 0) {
```

### NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=127">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=127</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c
Line	1871	1926
Object	null	key

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c  
Method ngx\_http\_uwsgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_uwsgi\_loc\_conf\_t \*conf,

```
....  
1871.         src = NULL;  
....  
1926.         if (src[i].key.len > sizeof("HTTP_") - 1
```

### NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=128">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=128</a>
Status	New



The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826 is not initialized when it is used by key at reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c in line 1826.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c
Line	1871	1927
Object	null	key

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c

Method ngx\_http\_uwsgi\_init\_params(ngx\_conf\_t \*cf, ngx\_http\_uwsgi\_loc\_conf\_t \*conf,

```
....
1871.             src = NULL;
....
1927.             && ngx_strcmp(src[i].key.data, "HTTP_",
sizeof("HTTP_") - 1) == 0)
```

#### NULL Pointer Dereference\Path 32:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=129>

Status New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_resolver.c in line 1421 is not initialized when it is used by addr6 at reading-code-of-nginx-1.9.2/nginx\_resolver.c in line 1421.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_resolver.c	reading-code-of-nginx-1.9.2/nginx_resolver.c
Line	1763	1814
Object	null	addr6

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_resolver.c

Method ngx\_resolver\_process\_a(ngx\_resolver\_t \*r, u\_char \*buf, size\_t last,

```
....
1763.             addr6 = NULL;
....
1814.             ngx_memcpy(addr6[n].s6_addr, &buf[i], 16);
```

#### NULL Pointer Dereference\Path 33:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=129>

Status	<a href="#">78&amp;pathid=130</a> New
--------	--

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 964 is not initialized when it is used by read at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 964.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	979	1020
Object	null	read

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_process(ngx\_stream\_session\_t \*s, ngx\_uint\_t from\_upstream,

```
....
979.         pc = u->upstream_buf.start ? u->peer.connection : NULL;
....
1020.         if (size && src->read->ready) {
```

#### NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=131">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=131</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 964 is not initialized when it is used by write at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 964.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	979	998
Object	null	write

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_process(ngx\_stream\_session\_t \*s, ngx\_uint\_t from\_upstream,

```
....
979.         pc = u->upstream_buf.start ? u->peer.connection : NULL;
....
998.         if (size && dst && dst->write->ready) {
```

#### NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=132">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=132</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 964 is not initialized when it is used by read at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 964.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	979	1051
Object	null	read

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_process(ngx\_stream\_session\_t \*s, ngx\_uint\_t from\_upstream,

```
....  
979.      pc = u->upstream_buf.start ? u->peer.connection : NULL;  
....  
1051.     if (src->read->eof && (b->pos == b->last || (dst && dst->read->eof))) {
```

#### NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=133">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=133</a>
Status	New

The variable declared in null at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 964 is not initialized when it is used by read at reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c in line 964.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_stream_proxy_module.c
Line	979	1051
Object	null	read

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_proxy\_module.c  
Method ngx\_stream\_proxy\_process(ngx\_stream\_session\_t \*s, ngx\_uint\_t from\_upstream,

```

.....
979.         pc = u->upstream_buf.start ? u->peer.connection : NULL;
.....
1051.        if (src->read->eof && (b->pos == b->last || (dst && dst-
>read->eof))) {

```

### NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=134">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=134</a>
Status	New

The variable declared in 0 at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 3234 is not initialized when it is used by b at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 3234.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	3294	3294
Object	0	b

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_send\_response(ngx\_http\_request\_t \*r, ngx\_uint\_t status, //status????????????????????4????ngx\_http\_status\_lines

```

.....
3294.         b->memory = val.len ? 1 : 0;

```

### NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=135">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=135</a>
Status	New

The variable declared in 0 at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 3234 is not initialized when it is used by b at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 3234.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	3295	3295
Object	0	b

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_send\_response(ngx\_http\_request\_t \*r, ngx\_uint\_t status, //status????????????????????4????nginx\_http\_status\_lines

```
....
3295.          b->last_buf = (r == r->main) ? 1 : 0;
```

### NULL Pointer Dereference\Path 39:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=136>  
Status New

The variable declared in 0 at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 6563 is not initialized when it is used by clcf at reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c in line 6563.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	6622	6622
Object	0	clcf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_root(ngx\_conf\_t \*cf, ngx\_command\_t \*cmd, void \*conf)

```
....
6622.          clcf->alias = alias ? clcf->name.len : 0;
```

### NULL Pointer Dereference\Path 40:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=137>  
Status New

The variable declared in 0 at reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c in line 201 is not initialized when it is used by b at reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c in line 201.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c
Line	369	369
Object	0	b

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c  
Method ngx\_http\_echo\_parse\_subrequest\_spec(ngx\_http\_request\_t \*r,

```
....
369.          b->in_file = b->file_last ? 1: 0;
```

#### NULL Pointer Dereference\Path 41:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=138>  
Status New

The variable declared in 0 at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1271 is not initialized when it is used by br at reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c in line 1271.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	1464	1463
Object	0	br

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_create\_request(ngx\_http\_request\_t \*r)  
//ngx\_http\_upstream\_init\_request

```
....
1464.          flcf->keep_conn ? NGX_HTTP_FASTCGI_KEEP_CONN : 0;
....
1463.          ngx_http_fastcgi_request_start.br.flags =
```

#### NULL Pointer Dereference\Path 42:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=139>  
Status New

The variable declared in 0 at reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c in line 961 is not initialized when it is used by stream at reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c in line 961.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_spdy.c	reading-code-of-nginx-1.9.2/nginx_http_spdy.c
Line	1035	1035
Object	0	stream

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c  
Method ngx\_http\_spdy\_state\_syn\_stream(ngx\_http\_spdy\_connection\_t \*sc, u\_char \*pos,

```
.....
1035.         stream->in_closed = (sc->flags & NGX_SPDY_FLAG_FIN) ? 1 : 0;
```

#### NULL Pointer Dereference\Path 43:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=140>  
Status New

The variable declared in 0 at reading-code-of-nginx-1.9.2/nginx\_resolver.c in line 470 is not initialized when it is used by rn at reading-code-of-nginx-1.9.2/nginx\_resolver.c in line 470.

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_resolver.c	reading-code-of-nginx-1.9.2/nginx_resolver.c
Line	658	658
Object	0	rn

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_resolver.c  
Method ngx\_resolve\_name\_locked(ngx\_resolver\_t \*r, ngx\_resolver\_ctx\_t \*ctx)

```
.....
658.         rn->naddrs6 = r->ipv6 ? (u_short) -1 : 0;
```

## 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=1050088&projectid=50078&pathid=67>  
Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	3956	3956

Object	sizeof	sizeof
--------	--------	--------

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c

Method ngx\_http\_subrequest(ngx\_http\_request\_t \*r,

```
....
3956.         sr->ctx = ngx_palloc(r->pool, sizeof(void *) *
ngx_http_max_module);
```

#### Use of Sizeof On a Pointer Type\Path 2:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=68>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	4134	4134
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c

Method ngx\_http\_internal\_redirect(ngx\_http\_request\_t \*r,

```
....
4134.         ngx_memzero(r->ctx, sizeof(void *) * ngx_http_max_module);
```

#### Use of Sizeof On a Pointer Type\Path 3:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=69>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	4208	4208
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c

Method ngx\_http\_named\_location(ngx\_http\_request\_t \*r, ngx\_str\_t \*name)



```
....
4208.          ngx_memzero(r->ctx, sizeof(void *) *
ngx_http_max_module);
```

#### Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=70">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=70</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	4517	4517
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_server(ngx\_conf\_t \*cf, ngx\_command\_t \*cmd, void \*dummy)

```
....
4517.      ctx->srv_conf = ngx_pcalloc(cf->pool, sizeof(void *) *
ngx_http_max_module);
```

#### Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=71">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=71</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	4524	4524
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_server(ngx\_conf\_t \*cf, ngx\_command\_t \*cmd, void \*dummy)

```
....
4524.      ctx->loc_conf = ngx_pcalloc(cf->pool, sizeof(void *) *
ngx_http_max_module);
```

**Use of Sizeof On a Pointer Type\Path 6:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=72">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=72</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	5053	5053
Object	sizeof	sizeof

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_location(ngx\_conf\_t \*cf, ngx\_command\_t \*cmd, void \*dummy)

```
....  
5053.         ctx->loc_conf = ngx_pcalloc(cf->pool, sizeof(void *) *  
ngx_http_max_module);
```

**Use of Sizeof On a Pointer Type\Path 7:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=73">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=73</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	5471	5471
Object	sizeof	sizeof

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method ngx\_http\_core\_create\_main\_conf(ngx\_conf\_t \*cf)

```
....  
5471.         sizeof(ngx_http_core_srv_conf_t *))
```

**Use of Sizeof On a Pointer Type\Path 8:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=74">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=74</a>

Status	<a href="#">78&amp;pathid=74</a> New
--------	---

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	6736	6736
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c

Method ngx\_http\_core\_limit\_except(ngx\_conf\_t \*cf, ngx\_command\_t \*cmd, void \*conf)

```
....  
6736.         ctx->loc_conf = ngx_palloc(cf->pool, sizeof(void *) *  
ngx_http_max_module);
```

#### Use of Sizeof On a Pointer Type\Path 9:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=75>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_echo_subrequest.c
Line	687	687
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_echo\_subrequest.c

Method ngx\_http\_echo\_exec\_exec(ngx\_http\_request\_t \*r,

```
....  
687.         ngx_memzero(r->ctx, sizeof(void *) * ngx_http_max_module);
```

#### Use of Sizeof On a Pointer Type\Path 10:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=76>

Status New

	Source	Destination
File	reading-code-of-nginx-	reading-code-of-nginx-

	1.9.2/nginx_http_fastcgi_module.c	1.9.2/nginx_http_fastcgi_module.c
Line	1355	1355
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_create\_request(ngx\_http\_request\_t \*r)  
//ngx\_http\_upstream\_init\_request??□?иú??

```
....  
1355.                ignored = ngx_palloc(r->pool, n * sizeof(void *));  
//□□□□h□□ ignored □□□□
```

#### Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=77">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=77</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	3258	3258
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_create\_main\_conf(ngx\_conf\_t \*cf)

```
....  
3258.                sizeof(ngx_http_file_cache_t *))
```

#### Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=78">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=78</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c
Line	188	188
Object	sizeof	sizeof

## Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_lua\_subrequest.c  
Method ngx\_http\_lua\_ngx\_location\_capture\_multi(lua\_State \*L)

```
....  
188.         sr_headers_len = nsubreqs * sizeof(ngx_http_headers_out_t);
```

**Use of Sizeof On a Pointer Type\Path 13:**

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=79>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c
Line	531	531
Object	sizeof	sizeof

## Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_lua\_subrequest.c  
Method ngx\_http\_lua\_ngx\_location\_capture\_multi(lua\_State \*L)

```
....  
531.         ofs1 = ngx_align(sizeof(ngx_http_post_subrequest_t),  
sizeof(void *));
```

**Use of Sizeof On a Pointer Type\Path 14:**

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=80>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c
Line	532	532
Object	sizeof	sizeof

## Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_lua\_subrequest.c  
Method ngx\_http\_lua\_ngx\_location\_capture\_multi(lua\_State \*L)

```
....
532.         ofs2 = ngx_align(sizeof(ngx_http_lua_ctx_t), sizeof(void
*)) );
```

#### Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=81">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=81</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c
Line	547	547
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_lua\_subrequest.c  
Method ngx\_http\_lua\_ngx\_location\_capture\_multi(lua\_State \*L)

```
....
547.     sizeof(void *));
```

#### Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=82">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=82</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c
Line	554	554
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_lua\_subrequest.c  
Method ngx\_http\_lua\_ngx\_location\_capture\_multi(lua\_State \*L)

```
....
554.     sizeof(void *));
```

**Use of Sizeof On a Pointer Type\Path 17:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=83">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=83</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c	reading-code-of-nginx-1.9.2/nginx_http_lua_subrequest.c
Line	1485	1485
Object	sizeof	sizeof

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/nginx\_http\_lua\_subrequest.c  
Method ngx\_http\_lua\_subrequest(ngx\_http\_request\_t \*r,

```
....  
1485.         sr->ctx = ngx_pcalloc(r->pool, sizeof(void *) *  
ngx_http_max_module);
```

**Use of Sizeof On a Pointer Type\Path 18:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=84">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=84</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_http_proxy_module.c
Line	3523	3523
Object	sizeof	sizeof

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/nginx\_http\_proxy\_module.c  
Method ngx\_http\_proxy\_create\_main\_conf(ngx\_conf\_t \*cf)

```
....  
3523.         sizeof(ngx_http_file_cache_t *))
```

**Use of Sizeof On a Pointer Type\Path 19:**

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=84">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=84</a>

Status	<a href="#">78&amp;pathid=85</a> New
--------	---

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_spdy.c	reading-code-of-nginx-1.9.2/nginx_http_spdy.c
Line	483	483
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c  
Method ngx\_http\_spdy\_init(ngx\_event\_t \*rev)

```
....  
483.                                     *  
sizeof(ngx_http_spdy_stream_t *));
```

#### Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=86">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=86</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_spdy.c	reading-code-of-nginx-1.9.2/nginx_http_spdy.c
Line	1159	1159
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c  
Method ngx\_http\_spdy\_state\_headers(ngx\_http\_spdy\_connection\_t \*sc, u\_char \*pos,

```
....  
1159.                                sizeof(ngx_table_elt_t *))
```

#### Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=87">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=87</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-	reading-code-of-nginx-



	1.9.2/nginx_http_spdy.c	1.9.2/nginx_http_spdy.c
Line	3535	3535
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c  
Method ngx\_http\_spdy\_keepalive\_handler(ngx\_event\_t \*rev)

```
....  
3535.                                     *  
sizeof(ngx_http_spdy_stream_t *));
```

#### Use of Sizeof On a Pointer Type\Path 22:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=88>  
Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_ssi_filter_module.c	reading-code-of-nginx-1.9.2/nginx_http_ssi_filter_module.c
Line	797	797
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_ssi\_filter\_module.c  
Method ngx\_http\_ssi\_body\_filter(ngx\_http\_request\_t \*r, ngx\_chain\_t \*in)

```
....  
797.                                     (NGX_HTTP_SSI_MAX_PARAMS + 1) *  
sizeof(ngx_str_t *));
```

#### Use of Sizeof On a Pointer Type\Path 23:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=89>  
Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_ssi_filter_module.c	reading-code-of-nginx-1.9.2/nginx_http_ssi_filter_module.c
Line	1750	1750
Object	sizeof	sizeof

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/nginx\_http\_ssi\_filter\_module.c

Method ngx\_http\_ssi\_evaluate\_string(ngx\_http\_request\_t \*r, ngx\_http\_ssi\_ctx\_t \*ctx,

```
....  
1750.      if (ngx_array_init(&lengths, r->pool, 8, sizeof(size_t *)) !=  
NGX_OK) {
```

**Use of Sizeof On a Pointer Type\Path 24:**

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=90>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_ssi_filter_module.c	reading-code-of-nginx-1.9.2/nginx_http_ssi_filter_module.c
Line	1754	1754
Object	sizeof	sizeof

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/nginx\_http\_ssi\_filter\_module.c

Method ngx\_http\_ssi\_evaluate\_string(ngx\_http\_request\_t \*r, ngx\_http\_ssi\_ctx\_t \*ctx,

```
....  
1754.      if (ngx_array_init(&values, r->pool, 8, sizeof(u_char *)) !=  
NGX_OK) {
```

**Use of Sizeof On a Pointer Type\Path 25:**

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=91>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c
Line	879	879
Object	sizeof	sizeof

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c

Method ngx\_http\_uwsgi\_create\_request(ngx\_http\_request\_t \*r)

```
.....
879.                ignored = ngx_palloc(r->pool, n * sizeof(void *));
```

### Use of Sizeof On a Pointer Type\Path 26:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=92">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=92</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c
Line	1360	1360
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c  
 Method ngx\_http\_uwsgi\_create\_main\_conf(ngx\_conf\_t \*cf)

```
.....
1360.                sizeof(ngx_http_file_cache_t *))
```

### Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=93">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=93</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_mail_core_module.c	reading-code-of-nginx-1.9.2/nginx_mail_core_module.c
Line	130	130
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_mail\_core\_module.c  
 Method ngx\_mail\_core\_create\_main\_conf(ngx\_conf\_t \*cf)

```
.....
130.                sizeof(ngx_mail_core_srv_conf_t *))
```

### Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
----------	-----

Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=94">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=94</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_mail_core_module.c	reading-code-of-nginx-1.9.2/nginx_mail_core_module.c
Line	235	235
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_mail\_core\_module.c

Method ngx\_mail\_core\_server(ngx\_conf\_t \*cf, ngx\_command\_t \*cmd, void \*conf)

```
....  
235.         ctx->srv_conf = ngx_palloc(cf->pool, sizeof(void *) *  
ngx_mail_max_module);
```

#### Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=95">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=95</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_mail_handler.c	reading-code-of-nginx-1.9.2/nginx_mail_handler.c
Line	361	361
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_mail\_handler.c

Method ngx\_mail\_init\_session(ngx\_connection\_t \*c)

```
....  
361.         s->ctx = ngx_palloc(c->pool, sizeof(void *) *  
ngx_mail_max_module);
```

#### Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=96">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=96</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_upstream.c	reading-code-of-nginx-1.9.2/nginx_stream_upstream.c
Line	110	110
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_upstream.c  
Method ngx\_stream\_upstream(ngx\_conf\_t \*cf, ngx\_command\_t \*cmd, void \*dummy)

```
....
110.                                     sizeof(void *) *
ngx_stream_max_module);
```

### Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=97">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=97</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_upstream.c	reading-code-of-nginx-1.9.2/nginx_stream_upstream.c
Line	431	431
Object	sizeof	sizeof

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_upstream.c  
Method ngx\_stream\_upstream\_create\_main\_conf(ngx\_conf\_t \*cf)

```
....
431.                                     sizeof(ngx_stream_upstream_srv_conf_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	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=97">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=97</a>

Status	<a href="#">78&amp;pathid=141</a> New
--------	--

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	58	58
Object	BC_FORL	BC_FORL

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_init(GG\_State \*GG)

```
....  
58.     disp[BC_FORL] = disp[BC_IFORL];
```

#### Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=142">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=142</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	59	59
Object	BC_ITERL	BC_ITERL

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_init(GG\_State \*GG)

```
....  
59.     disp[BC_ITERL] = disp[BC_IITERL];
```

#### Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=143">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=143</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c

Line	60	60
Object	BC_LOOP	BC_LOOP

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c

Method void lj\_dispatch\_init(GG\_State \*GG)

```
....
60.     disp[BC_LOOP] = disp[BC_ILOOP];
```

#### Unchecked Array Index\Path 4:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=144>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	136	136
Object	BC_RETM	BC_RETM

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c

Method void lj\_dispatch\_update(global\_State \*g)

```
....
136.         disp[BC_RETM] = lj_vm_rethook;
```

#### Unchecked Array Index\Path 5:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=145>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	137	137
Object	BC_RET	BC_RET

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c

Method void lj\_dispatch\_update(global\_State \*g)

```
....  
137.          disp[BC_RET] = lj_vm_rethook;
```

#### Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=146">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=146</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	138	138
Object	BC_RET0	BC_RET0

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
....  
138.          disp[BC_RET0] = lj_vm_rethook;
```

#### Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=147">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=147</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	139	139
Object	BC_RET1	BC_RET1

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
....  
139.          disp[BC_RET1] = lj_vm_rethook;
```

#### Unchecked Array Index\Path 8:



Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=148">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=148</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	150	150
Object	BC_FORL	BC_FORL

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
....  
150.         disp[BC_FORL] = f_forl;
```

#### Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=149">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=149</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	151	151
Object	BC_ITERL	BC_ITERL

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
....  
151.         disp[BC_ITERL] = f_iterl;
```

#### Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=150">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=150</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	152	152
Object	BC_LOOP	BC_LOOP

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
....  
152.         disp[BC_LOOP] = f_loop;
```

#### Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=151">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=151</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	155	155
Object	BC_RETM	BC_RETM

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
....  
155.         disp[BC_RETM] = lj_vm_rethook;
```

#### Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=152">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=152</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	156	156

Object	BC_RET	BC_RET
--------	--------	--------

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c

Method void lj\_dispatch\_update(global\_State \*g)

```
....  
156.         disp[BC_RET] = lj_vm_rethook;
```

**Unchecked Array Index\Path 13:**

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=153>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	157	157
Object	BC_RET0	BC_RET0

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c

Method void lj\_dispatch\_update(global\_State \*g)

```
....  
157.         disp[BC_RET0] = lj_vm_rethook;
```

**Unchecked Array Index\Path 14:**

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=154>

Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	158	158
Object	BC_RET1	BC_RET1

**Code Snippet**

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c

Method void lj\_dispatch\_update(global\_State \*g)

```
.....
158.          disp[BC_RET1] = lj_vm_rethook;
```

#### Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=155">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=155</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	160	160
Object	BC_RETM	BC_RETM

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
.....
160.          disp[BC_RETM] = disp[GG_LEN_DDISP+BC_RETM];
```

#### Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=156">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=156</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	161	161
Object	BC_RET	BC_RET

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
.....
161.          disp[BC_RET] = disp[GG_LEN_DDISP+BC_RET];
```

#### Unchecked Array Index\Path 17:

Severity	Low
----------	-----

Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=157">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=157</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	162	162
Object	BC_RET0	BC_RET0

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
....  
162.         disp[BC_RET0] = disp[GG_LEN_DDISP+BC_RET0];
```

#### Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=158">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=158</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_dispatch.c	reading-code-of-nginx-1.9.2/lj_dispatch.c
Line	163	163
Object	BC_RET1	BC_RET1

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_dispatch.c  
Method void lj\_dispatch\_update(global\_State \*g)

```
....  
163.         disp[BC_RET1] = disp[GG_LEN_DDISP+BC_RET1];
```

#### Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=159">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=159</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	2413	2413
Object	len	len

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_process\_header(ngx\_http\_request\_t \*r)

```
.....  
2413.                                h->value.data[h->value.len] = '\0';
```

#### Unchecked Array Index\Path 20:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=160>  
Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_fastcgi_module.c
Line	2440	2440
Object	len	len

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_fastcgi\_module.c  
Method ngx\_http\_fastcgi\_process\_header(ngx\_http\_request\_t \*r)

```
.....  
2440.                                h->value.data[h->value.len] = '\0';
```

#### Unchecked Array Index\Path 21:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=161>  
Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_lua_headers.c	reading-code-of-nginx-1.9.2/nginx_http_lua_headers.c
Line	835	835

Object	len	len
--------	-----	-----

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_lua\_headers.c  
Method ngx\_http\_lua\_ngx\_req\_header\_set\_helper(lua\_State \*L)

```
....  
835.         key.data[len] = '\0';
```

#### Unchecked Array Index\Path 22:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=162>  
Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_lua_headers.c	reading-code-of-nginx-1.9.2/nginx_http_lua_headers.c
Line	1214	1214
Object	key_len	key_len

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_lua\_headers.c  
Method ngx\_http\_lua\_ffi\_req\_header\_set\_single\_value(ngx\_http\_request\_t \*r,

```
....  
1214.         k.data[key_len] = '\0';
```

#### Unchecked Array Index\Path 23:

Severity Low  
Result State To Verify  
Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=163>  
Status New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_proxy_module.c	reading-code-of-nginx-1.9.2/nginx_http_proxy_module.c
Line	2525	2525
Object	len	len

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_proxy\_module.c  
Method ngx\_http\_proxy\_process\_header(ngx\_http\_request\_t \*r)

```
.....
2525.          h->value.data[h->value.len] = '\0';
```

#### Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=164">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=164</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_spdy.c	reading-code-of-nginx-1.9.2/nginx_http_spdy.c
Line	2473	2473
Object	index	index

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_spdy.c  
Method ngx\_http\_spdy\_create\_stream(ngx\_http\_spdy\_connection\_t \*sc, ngx\_uint\_t id,

```
.....
2473.          sc->streams_index[index] = stream;
```

#### Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=165">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=165</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c	reading-code-of-nginx-1.9.2/nginx_http_uwsgi_module.c
Line	1240	1240
Object	len	len

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_uwsgi\_module.c  
Method ngx\_http\_uwsgi\_process\_header(ngx\_http\_request\_t \*r)

```
.....
1240.          h->value.data[h->value.len] = '\0';
```

#### Unchecked Array Index\Path 26:

Severity	Low
----------	-----



Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=166">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=166</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_stream_upstream.c	reading-code-of-nginx-1.9.2/nginx_stream_upstream.c
Line	115	115
Object	ctx_index	ctx_index

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_stream\_upstream.c  
 Method ngx\_stream\_upstream(ngx\_conf\_t \*cf, ngx\_command\_t \*cmd, void \*dummy)

```
....
115.      ctx->srv_conf[ngx_stream_upstream_module.ctx_index] = uscf;
```

## Information Exposure Through Comments

Query Path:

CPP\Cx\CPP Low Visibility\Information Exposure Through Comments Version:1

### Categories

FISMA 2014: Identification And Authentication

NIST SP 800-53: SC-28 Protection of Information at Rest (P1)









































### Description

#### Information Exposure Through Comments\Path 1:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=52">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=52</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_event_openssl.c	reading-code-of-nginx-1.9.2/nginx_event_openssl.c
Line	1141	1141
Object	cipher:	cipher:

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_event\_openssl.c  
 Method /\*                                           

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=53">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=53</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2378	2378
Object	cipher-	cipher-

File Name	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Method	try_files index_large.html gmime-gmime-cipher-context.html;:

```
....
2378. 00000000:try_files index_large.html gmime-gmime-cipher-
context.html;00 00030000:
```

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=54">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=54</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2380	2380
Object	cipher-	cipher-

```
File Name  reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Method     trying to use file: "gmime-gmime-cipher-context.html"
           "/usr/local/nginx/htmlgmime-gmime-cipher-context.html"
           ██████████
```

```
....
2380.  trying to use file: "gmime-gmime-cipher-context.html"
"/usr/local/nginx/htmlgmime-gmime-cipher-context.html"  □□□□↓□□□□Dz□□□□□
```

#### Information Exposure Through Comments\Path 4:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=55">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=55</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2380	2380
Object	cipher-	cipher-

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
 Method trying to use file: "gmime-gmime-cipher-context.html"  
 "/usr/local/nginx/htmlgmime-gmime-cipher-context.html"  
 ??????j?????□??????

```
....
2380.  trying to use file: "gmime-gmime-cipher-context.html"
"/usr/local/nginx/htmlgmime-gmime-cipher-context.html"  □□□□↓□□□□Dz□□□□□
```

#### Information Exposure Through Comments\Path 5:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=56">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=56</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2381	2381
Object	cipher-	cipher-

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
 Method internal redirect: "gmime-gmime-cipher-context.html?"  
 ??????ض?????uri□?İ????????□?try\_files?j?

```
....
2381. internal redirect: "gmime-gmime-cipher-context.html?"
0x00000000uri0000i00000000N0try_files010
```

### Information Exposure Through Comments\Path 6:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=57">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=57</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2383	2383
Object	cipher-	cipher-

Code Snippet

File Name	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Method	find config phase: 1 (NGX_HTTP_FIND_CONFIG_PHASE), uri:gmime-gmime-cipher-context.html

```
....
2383. find config phase: 1 (NGX_HTTP_FIND_CONFIG_PHASE), uri:gmime-
gmime-cipher-context.html
```

### Information Exposure Through Comments\Path 7:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=58">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=58</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2386	2386
Object	cipher-	cipher-

## Code Snippet

File Name	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Method	try_files /index_large.html gmime-gmime-cipher-context.html;

```
....
2386.  :try_files /index_large.html gmime-gmime-cipher-
context.html;
```

### Information Exposure Through Comments\Path 8:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=59">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=59</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2505	2505
Object	cipher-	cipher-

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method :try\_files index\_large.html gmime-gmime-cipher-context.html;

```
....
2505.  :try_files index_large.html gmime-gmime-cipher-
context.html;
```

### Information Exposure Through Comments\Path 9:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=60">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=60</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2507	2507
Object	cipher-	cipher-

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method trying to use file: "gmime-gmime-cipher-context.html"  
"/usr/local/nginx/htmlgmime-gmime-cipher-context.html"

```
.....
2507.  trying to use file: "gmime-gmime-cipher-context.html"
"/usr/local/nginx/htmlgmime-gmime-cipher-context.html"  □□□□↓□□□□Dz□□□□□
```

### Information Exposure Through Comments\Path 10:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=61">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=61</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2507	2507
Object	cipher-	cipher-

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method trying to use file: "gmime-gmime-cipher-context.html"  
"/usr/local/nginx/htmlgmime-gmime-cipher-context.html"  
?????j?????□??????

```
.....
2507.  trying to use file: "gmime-gmime-cipher-context.html"
"/usr/local/nginx/htmlgmime-gmime-cipher-context.html"  □□□□↓□□□□Dz□□□□□
```

### Information Exposure Through Comments\Path 11:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=62">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=62</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2508	2508
Object	cipher-	cipher-

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c  
Method internal redirect: "gmime-gmime-cipher-context.html?"  
?????ض?????uri□?İ?????□?try\_files?j?

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=63">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=63</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2510	2510
Object	cipher-	cipher-

File Name	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Method	find config phase: 1 (NGX_HTTP_FIND_CONFIG_PHASE), uri:gmime-gmime-cipher-context.html

```
....
2510. find config phase: 1 (NGX_HTTP_FIND_CONFIG_PHASE), uri:gmime-
gmime-cipher-context.html
```

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=64">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=64</a>
Status	New

	Source	Destination
File	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	2513	2513
Object	cipher-	cipher-

File Name	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Method	try_files /index_large.html gmime-gmime-cipher-context.html;

```
....
2513. 00000000:try_files /index_large.html gmime-gmime-cipher-
context.html;
```

## Potential Off by One Error in Loops

Query Path:

CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection

NIST SP 800-53: SI-16 Memory Protection (P1)

OWASP Top 10 2017: A1-Injection

### Description

#### Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=2">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=2</a>
Status	New

The buffer allocated by <= in reading-code-of-nginx-1.9.2/lj\_gc.c at line 157 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_gc.c	reading-code-of-nginx-1.9.2/lj_gc.c
Line	189	189
Object	<=	<=

### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_gc.c  
Method static int gc\_traverse\_tab(global\_State \*g, GCtab \*t)

```
....
189.     for (i = 0; i <= hmask; i++) {
```

#### Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=3">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=3</a>
Status	New

The buffer allocated by <= in reading-code-of-nginx-1.9.2/lj\_gc.c at line 428 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

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



File	reading-code-of-nginx-1.9.2/lj_gc.c	reading-code-of-nginx-1.9.2/lj_gc.c
Line	445	445
Object	<=	<=

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_gc.c  
Method static void gc\_clearweak(GCobj \*o)

```
....  
445.      for (i = 0; i <= hmask; i++) {
```

### Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=4">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=4</a>
Status	New

The buffer allocated by <= in reading-code-of-nginx-1.9.2/lj\_gc.c at line 555 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	reading-code-of-nginx-1.9.2/lj_gc.c	reading-code-of-nginx-1.9.2/lj_gc.c
Line	562	562
Object	<=	<=

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/lj\_gc.c  
Method void lj\_gc\_freeall(global\_State \*g)

```
....  
562.      for (i = 0; i <= strmask; i++) /* Free all string hash chains.  
*/
```

## 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	<a href="http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=65">http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&amp;projectid=50078&amp;pathid=65</a>
Status	New

The ngx\_http\_phase\_2str method calls the snprintf function, at line 1845 of reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.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	reading-code-of-nginx-1.9.2/nginx_http_core_module.c	reading-code-of-nginx-1.9.2/nginx_http_core_module.c
Line	1886	1886
Object	snprintf	snprintf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_http\_core\_module.c

Method const char\* ngx\_http\_phase\_2str(ngx\_uint\_t phase)

```
....
1886.      snprintf(buf, sizeof(buf), "error phase:%u", (unsigned
int)phase);
```

#### Unchecked Return Value\Path 2:

Severity Low

Result State To Verify

Online Results <http://WIN-BA8RD5TJ8IG/CxWebClient/ViewerMain.aspx?scanid=1050088&projectid=50078&pathid=66>

Status New

The ngx\_udp\_connect method calls the snprintf function, at line 3044 of reading-code-of-nginx-1.9.2/nginx\_resolver.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	reading-code-of-nginx-1.9.2/nginx_resolver.c	reading-code-of-nginx-1.9.2/nginx_resolver.c
Line	3115	3115
Object	snprintf	snprintf

#### Code Snippet

File Name reading-code-of-nginx-1.9.2/nginx\_resolver.c

Method ngx\_udp\_connect(ngx\_udp\_connection\_t \*uc)

```
....
3115.      snprintf(tmpbuf, sizeof(tmpbuf), "<%25s, %5d> epoll
NGX_READ_EVENT(et) read add", NGX_FUNC_LINE);
```

## Format String Attack

### Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

---

## Cause

### How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

---

## General Recommendations

### How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
  - Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.
- 

## Source Code Examples

### CPP

#### Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");  
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or  
cause a crash
```

### Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

# Buffer Overflow AddressOfLocalVarReturned

## Risk

### What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

---

## Cause

### How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

---

## General Recommendations

### How to avoid it

- Do not return local variables or pointers
  - Review code to ensure no flow allows use of a pointer after it has been explicitly freed
- 

## Source Code Examples

# Buffer Overflow boundcpy WrongSizeParam

## Risk

### What might happen

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

---

## Cause

### How does it happen

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

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

---

## General Recommendations

### How to avoid it

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

## Source Code Examples

### CPP

#### Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

#### Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

# Dangerous Functions

## Risk

### What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

---

## Cause

### How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

---

## General Recommendations

### How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
  - Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.
- 

## Source Code Examples

### CPP

#### Buffer Overflow in gets()

```
int main()
{
    char buf[10];

    printf("Please enter your name: ");
    gets(buf); // veryveryverylongname
    if (buf == ACCEPTED_NAME)
    {
        // Do something
    }
    return 0;
}
```



## Safe reading from user

```
int main()
{
    char buf[10];

    printf("Please enter your name: ");
    fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
    if (buf == ACCEPTED_NAME)
    {
        //Do something
    }
    return 0;
}
```

## Unsafe function for string copy

```
int main(int argc, char* argv[])
{
    char buf[10];
    strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

    return 0;
}
```

## Safe string copy

```
int main(int argc, char* argv[])
{
    char buf[10];
    strncpy(buf, argv[1], sizeof(buf));
    buf[9] = '\0'; //strncpy doesn't NULL terminates

    return 0;
}
```

## Unsafe format string

```
int main(int argc, char* argv[])
{
    printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause an access violation
    return 0;
}
```

## Safe format string

```
int main(int argc, char* argv[])
{
    printf("%s", argv[1]); // Second parameter is not a formattable string
    return 0;
}
```

# Heap Inspection

## Risk

### What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privileged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.

Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

---

## Cause

### How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

---

## General Recommendations

### How to avoid it

Generic Guidance:

- Do not store sensitive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as `SealedObject`.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as `SecureString` or `ProtectedData`.
- 

## Source Code Examples

### Java

#### Plaintext Password in Immutable String

```
class Heap_Inspection
{
    private string password;
```

```
void setPassword()  
{  
    password = System.console().readLine("Enter your password: ");  
}  
}
```

## Password Protected in Memory

```
class Heap_Inspection_Fixed  
{  
    private SealedObject password;  
  
    void setPassword()  
    {  
        byte[] sKey = getKeyFromConfig();  
        Cipher c = Cipher.getInstance("AES");  
        c.init(Cipher.ENCRYPT_MODE, sKey);  
  
        char[] input = System.console().readPassword("Enter your password: ");  
        password = new SealedObject(Arrays.asList(input), c);  
  
        //Zero out the possible password, for security.  
        Arrays.fill(password, '0');  
    }  
}
```

## CPP

### Vulnerable C code

```
/* Vulnerable to heap inspection */  
  
#include <stdio.h>  
  
void somefunc() {  
    printf("Yea, I'm just being called for the heap of it..\n");  
}  
  
void authfunc() {  
    char* password = (char *) malloc(256);  
    char ch;  
    ssize_t k;  
    int i=0;  
    while(k = read(0, &ch, 1) > 0)  
    {  
        if (ch == '\n') {  
            password[i]='\0';  
            break;  
        } else {  
            password[i++]=ch;  
            fflush(0);  
        }  
    }  
    printf("Password: %s\n", &password[0]);  
}
```

```
int main()
{
    printf("Please enter a password:\n");

    authfunc();
    printf("You can now dump memory to find this password!");
    somefunc();
    gets();
}
```

## Safe C code

```
/* Presumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc() {
    printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc() {
    char* password = (char*) malloc(256);
    int i=0;
    char ch;
    ssize_t k;
    while(k = read(STDIN_FILENO, &ch, 1) > 0)
    {
        if (ch == '\n') {
            password[i]='\0';
            break;
        } else {
            password[i++]=ch;
            fflush(0);
        }
    }
    i=0;
    memset(password, '\0', 256);
}

int main()
{
    printf("Please enter a password:\n");
    authfunc();
    somefunc();
    char ch;
    while(read(STDIN_FILENO, &ch, 1) > 0)
    {
        if (ch == '\n')
            break;
    }
}
```

## Failure to Release Memory Before Removing Last Reference ('Memory Leak')

**Weakness ID:** 401 (*Weakness Base*)

**Status:** Draft

### Description

#### Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

#### Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

#### Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

#### Time of Introduction

- Architecture and Design
- Implementation

#### Applicable Platforms

#### Languages

C

C++

#### Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

#### Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

#### Likelihood of Exploit

Medium

#### Demonstrative Examples

##### Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(*Bad Code*)

*Example Language: C*

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

## Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: C

```
bar connection(){
foo = malloc(1024);
return foo;
}

endConnection(bar foo) {

free(foo);
}

int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

## Observed Examples

Reference	Description
<a href="#">CVE-2005-3119</a>	Memory leak because function does not free() an element of a data structure.
<a href="#">CVE-2004-0427</a>	Memory leak when counter variable is not decremented.
<a href="#">CVE-2002-0574</a>	Memory leak when counter variable is not decremented.
<a href="#">CVE-2005-3181</a>	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
<a href="#">CVE-2004-0222</a>	Memory leak via unknown manipulations as part of protocol test suite.
<a href="#">CVE-2001-0136</a>	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	<a href="#">Indicator of Poor Code Quality</a>	<b>Seven Pernicious Kingdoms (primary)700</b>
ChildOf	Category	399	<a href="#">Resource Management Errors</a>	<b>Development Concepts (primary)699</b>
ChildOf	Category	633	<a href="#">Weaknesses that Affect Memory</a>	<b>Resource-specific Weaknesses (primary)631</b>
ChildOf	Category	730	<a href="#">OWASP Top Ten 2004 Category A9 - Denial of Service</a>	<b>Weaknesses in OWASP Top Ten (2004) (primary)711</b>
ChildOf	Weakness Base	772	<a href="#">Missing Release of Resource after Effective</a>	<b>Research Concepts (primary)1000</b>

MemberOf	View	630	<a href="#">Lifetime Weaknesses Examined by SAMATE</a>	<b>Weaknesses Examined by SAMATE (primary) 630</b> Research Concepts1000
CanFollow	Weakness Class	390	<a href="#">Detection of Error Condition Without Action</a>	

## 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 updated White Box Definitions	MITRE	Internal
2009-10-29	CWE Content Team updated Modes of Introduction, Other Notes	MITRE	Internal
2010-02-16	CWE Content Team updated Relationships	MITRE	Internal
<b>Previous Entry Names</b>			
<b>Change Date</b>	<b>Previous Entry Name</b>		
2008-04-11	Memory Leak		
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')		

[BACK TO TOP](#)

# Use After Free

## Risk

### What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

---

## Cause

### How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

---

## General Recommendations

### How to avoid it

- Do not return local variables or pointers
  - Review code to ensure no flow allows use of a pointer after it has been explicitly freed
- 

## Source Code Examples

### CPP

#### Use of Variable after It was Freed

```
free(input);  
printf("%s", input);
```

#### Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()  
{  
    int i;  
    i = 1;  
    return &i;  
}  
  
void func2()  
{  
    int j;  
    j = 5;
```

```
}  
  
//..  
    int * i = func1();  
    printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault  
    func2();  
    printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in  
the stack  
//..
```

# 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());
```



# Potential Off by One Error in Loops

## Risk

### What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

---

## Cause

### How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition `i=0` and the continuation condition `i<=2`, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

---

## General Recommendations

### How to avoid it

- Always ensure that a given iteration boundary is correct:
    - With array iterations, consider that arrays begin with cell 0 and end with cell `n-1`, for a size `n` array.
    - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
  - Where possible, use safe functions that manage memory and are not prone to off-by-one errors.
- 

## Source Code Examples

### CPP

#### Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
    ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
}
```

```
}
```

### Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
    ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

### Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf) -  
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

## Information Leak Through Comments

**Weakness ID:** 615 (*Weakness Variant*)

**Status:** Incomplete

### Description

#### Description Summary

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

#### Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

#### Time of Introduction

#### Implementation

#### Demonstrative Examples

##### Example 1

The following comment, embedded in a JSP, will be displayed in the resulting HTML output.

(Bad Code)

*Example Languages:* **HTML and JSP**

```
<!-- FIXME: calling this with more than 30 args kills the JDBC server -->
```

#### Observed Examples

Reference	Description
<a href="#">CVE-2007-6197</a>	Version numbers and internal hostnames leaked in HTML comments.
<a href="#">CVE-2007-4072</a>	CMS places full pathname of server in HTML comment.
<a href="#">CVE-2009-2431</a>	blog software leaks real username in HTML comment.

#### Potential Mitigations

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

#### Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Variant	540	Information Leak Through Source Code	<b>Development Concepts (primary)699</b> <b>Research Concepts (primary)1000</b>

#### Content History

Submissions			
Submission Date	Submitter	Organization	Source
	Anonymous Tool Vendor (under NDA)		Externally Mined
Modifications			
Modification Date	Modifier	Organization	Source
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal



	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Observed Examples, Taxonomy Mappings		

[BACK TO TOP](#)

# Unchecked Return Value

## Risk

### What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

---

## Cause

### How does it happen

The application calls a system function, but does not receive or check the result of this function. These functions often return error codes in the result, or share other status codes with its caller. The application simply ignores this result value, losing this vital information.

---

## General Recommendations

### How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.
  - Ensure the calling function responds to all possible return values.
  - Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.
- 

## Source Code Examples

### CPP

#### Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

#### Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

## Use of sizeof() on a Pointer Type

**Weakness ID:** 467 (*Weakness Variant*)

**Status:** Draft

### Description

### Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

### Time of Introduction

### Implementation

### Applicable Platforms

### Languages

C

C++

### Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

### Likelihood of Exploit

High

### Demonstrative Examples

#### Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

*(Bad Code)*

*Example Languages: C and C++*

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(\*foo) returns the size of the data structure and not the size of the pointer.

*(Good Code)*

*Example Languages: C and C++*

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

#### Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

*(Bad Code)*

*/\* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. \*/*

```
char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strcmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strcmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In `AuthenticateUser()`, because `sizeof()` is applied to a parameter with an array type, the `sizeof()` call might return 4 on many modern architectures. As a result, the `strcmp()` call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

*(Attack)*

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

## Potential Mitigations

### Phase: Implementation

Use expressions such as "`sizeof(*pointer)`" instead of "`sizeof(pointer)`", unless you intend to run `sizeof()` on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

## Other Notes

The use of `sizeof()` on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of `sizeof(pointer)` indicates a bug.

## Weakness Ordinalities

Ordinality	Description
Primary	(where the weakness exists independent of other weaknesses)

## Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	<a href="#">Pointer Issues</a>	<b>Development Concepts (primary)699</b>
ChildOf	Weakness Class	682	<a href="#">Incorrect Calculation</a>	<b>Research Concepts (primary)1000</b>
ChildOf	Category	737	<a href="#">CERT C Secure Coding Section 03 - Expressions (EXP)</a>	<b>Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734</b>
ChildOf	Category	740	<a href="#">CERT C Secure Coding Section 06 - Arrays (ARR)</a>	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	<a href="#">Incorrect Calculation of Buffer Size</a>	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](#)

# 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

## Improper Validation of Array Index

**Weakness ID:** 129 (*Weakness Base*)

**Status:** Draft

### Description

### Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

### Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

### Time of Introduction

### Implementation

### Applicable Platforms

### Languages

C: (*Often*)

C++: (*Often*)

### Language-independent

### Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

### Likelihood of Exploit

High

### Detection Methods

#### Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

**Effectiveness: High**

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

---

### Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

---

### Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

---

## Demonstrative Examples

### Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

*(Bad Code)*

*Example Language: C*

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
    ...
    char buf[BUFFER_SIZE];
    int ok;
    int num, size;

    // read values from socket and added to sizes array
    while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
    {

        // continue read from socket until buf only contains '.'
        if (DOTLINE(buf))
            break;
        else if (sscanf(buf, "%d %d", &num, &size) == 2)
            sizes[num - 1] = size;
        }
    ...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

*(Good Code)*

*Example Language: C*

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
    ...
    char buf[BUFFER_SIZE];
    int ok;
    int num, size;

    // read values from socket and added to sizes array
    while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
    {

        // continue read from socket until buf only contains '.'
        if (DOTLINE(buf))
```



```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

## Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

*(Bad Code)*

**Example Language: Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an `ArrayIndexOutOfBoundsException` Exception being raised.

## Example 3

In the following Java example the method `displayProductSummary` is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the `displayProductSummary` method. The `displayProductSummary` method passes the integer value of the product number to the `getProductSummary` method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

*(Bad Code)*

**Example Language: Java**

*// Method called from servlet to obtain product information*

```
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may cause the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

*(Good Code)*

**Example Language: Java**

*// Method called from servlet to obtain product information*

```
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as `ArrayList` that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

*(Good Code)*

#### Example Language: Java

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

### Observed Examples

Reference	Description
<a href="#">CVE-2005-0369</a>	large ID in packet used as array index
<a href="#">CVE-2001-1009</a>	negative array index as argument to POP LIST command
<a href="#">CVE-2003-0721</a>	Integer signedness error leads to negative array index
<a href="#">CVE-2004-1189</a>	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
<a href="#">CVE-2007-5756</a>	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	<a href="#">Improper Input Validation</a>	<b>Development Concepts (primary)699</b> <b>Research Concepts (primary)1000</b>
ChildOf	Category	189	<a href="#">Numeric Errors</a>	Development Concepts699
ChildOf	Category	633	<a href="#">Weaknesses that Affect Memory</a>	<b>Resource-specific Weaknesses (primary)631</b>
ChildOf	Category	738	<a href="#">CERT C Secure Coding Section 04 - Integers (INT)</a>	<b>Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734</b>
ChildOf	Category	740	<a href="#">CERT C Secure Coding Section 06 - Arrays (ARR)</a>	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	<a href="#">2010 Top 25 - Risky Resource Management</a>	<b>Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800</b>
CanPrecede	Weakness Class	119	<a href="#">Failure to Constrain Operations within the Bounds of a Memory Buffer</a>	Research Concepts1000
CanPrecede	Weakness Variant	789	<a href="#">Uncontrolled Memory Allocation</a>	Research Concepts1000
PeerOf	Weakness Base	124	<a href="#">Buffer Underwrite ('Buffer Underflow')</a>	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)
<a href="#">100</a>	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](#)

## Scanned Languages

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