# 漏洞扫描探测报告

报告时间：2024.11.10

# 1.综述

## 1.1 任务信息

本次任务发现 5 个资产，5 个存活 ip，9 个开放端口。

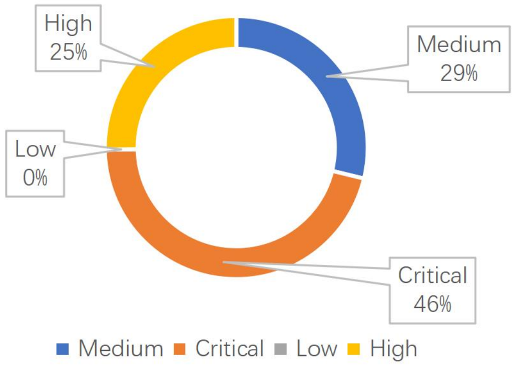
| | | | |
|---|---|---|---|
| 5 | 5 | 9 | 13 |
| 资产 | 存活 ip | 开放端口 | 漏洞 |

## 1.2 任务详情

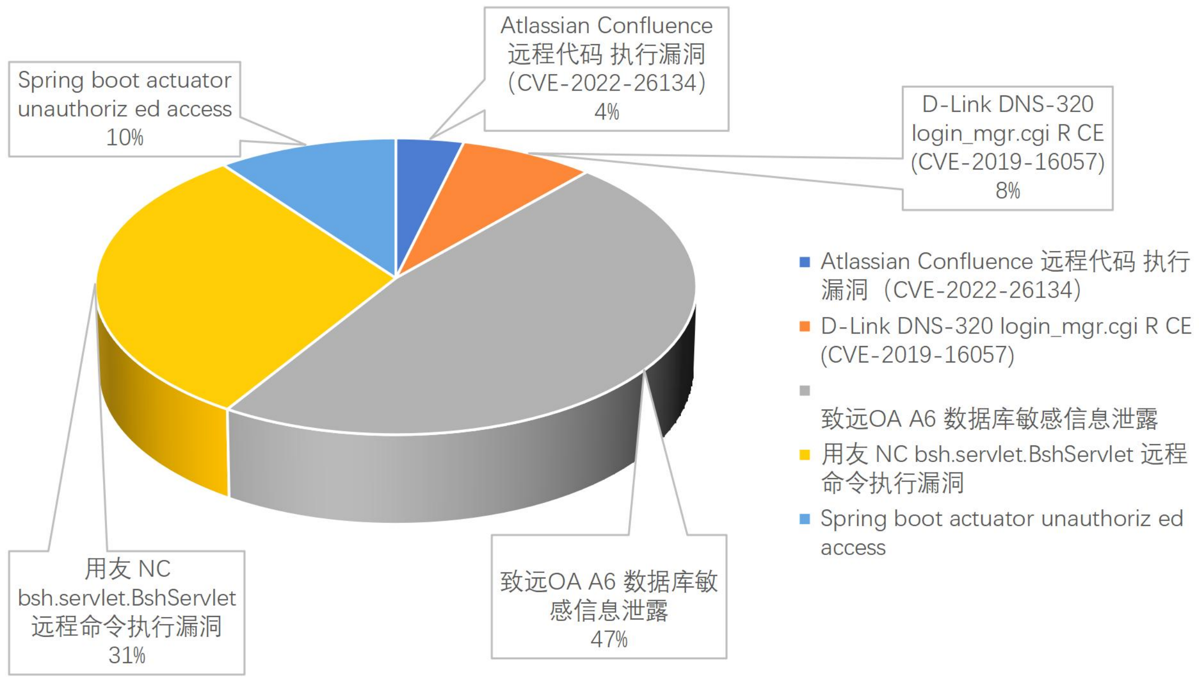
| | |
|---|---|
| IP/Domain | 153.153.1.0/24 |
| 端口 | 1-65535 |
| 漏洞 | 通用 PoC |
| 进度 | 100% |
| 开始时间 | 2024-11-10 |

## 1.3 风险分布

风险资产分布



风险统计（TOP5）



## 1.4 资产分布

### 1.4.1 IP 资产分布

■

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 |
| 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 |
| 58 | 59 | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 |
| 77 | 78 | 79 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 |
| 96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 | 104 | 105 | 106 | 107 | 108 | 109 | 110 | 111 | 112 | 113 | 114 |
| 115 | 116 | 117 | 118 | 119 | 120 | 121 | 122 | 123 | 124 | 125 | 126 | 127 | 128 | 129 | 130 | 131 | 132 | 133 |
| 134 | 135 | 136 | 137 | 138 | 139 | 140 | 141 | 142 | 143 | 144 | 145 | 146 | 147 | 148 | 149 | 150 | 151 | 152 |

全部 > 47.251.0.0 >47.251.44.0>

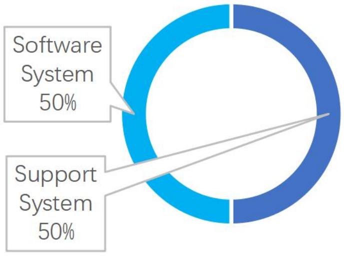
存活

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 153 | 154 | 155 | 156 | 157 | 158 | 159 | 160 | 161 | 162 | 163 | 164 | 165 | 166 | 167 | 168 | 169 | 170 | 171 |
| 172 | 173 | 174 | 175 | 176 | 177 | 178 | 179 | 180 | 181 | 182 | 183 | 184 | 185 | 186 | 187 | 188 | 189 | 190 |
| 191 | 192 | 193 | 194 | 195 | 196 | 197 | 198 | 199 | 200 | 201 | 202 | 203 | 204 | 205 | 206 | 207 | 208 | 209 |
| 210 | 211 | 212 | 213 | 214 | 215 | 216 | 217 | 218 | 219 | 220 | 221 | 222 | 223 | 224 | 225 | 226 | 227 | 228 |
| 229 | 230 | 231 | 232 | 233 | 234 | 235 | 236 | 237 | 238 | 239 | 240 | 241 | 242 | 243 | 244 | 245 | 246 | 247 |
| 248 | 249 | 250 | 251 | 252 | 253 | 254 | 255 | | | | | | | | | | | |

### 1.4.2 网络结构

# 暂无数据

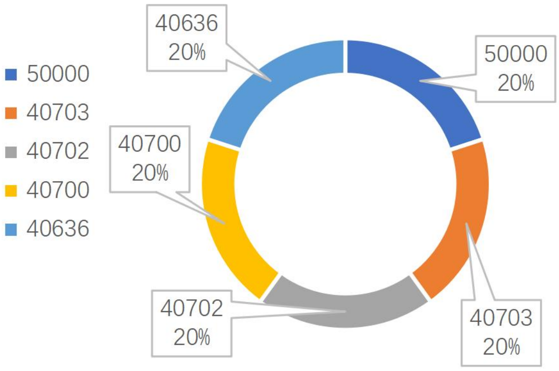
### 1.4.3 资产类型分布



| | | |
|---|---|---|
| Support System | 1 | 50.00% |
| Software System | 1 | 50.00% |

共有 2

### 1.4.4 端口开放情况



| | | |
|---|---|---|
| 50000 | 1 | 20.00% |
| 40703 | 1 | 20.00% |
| 40702 | 1 | 20.00% |
| 40700 | 1 | 20.00% |
| 40636 | 1 | 20.00% |

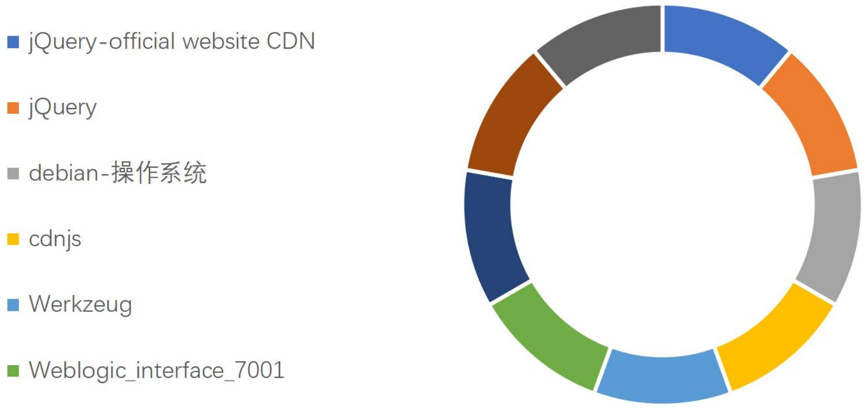
共有：5

## 2.资产分析

### 2.1 硬件

# 暂无数据

## 2.2 软件

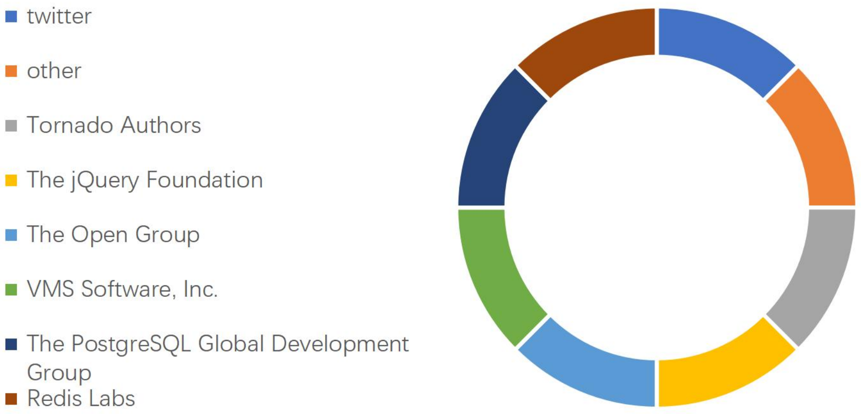


| | | |
|---|---|---|
| jQuery-official website CDN | 1 | 20.00% |
| jQuery | 1 | 20.00% |
| debian-操作系统 | 1 | 20.00% |
| cdnjs | 1 | 20.00% |
| Werkzeug | 1 | 20.00% |
| Weblogic_interface_7001 | 1 | 20.00% |
| VMS_Software-OpenVMS | 1 | 20.00% |
| Redis | 1 | 20.00% |
| PostgreSQL | 1 | 20.00% |
| 共有：9 | | |

## 2.3 硬件厂商

# 暂无数据

## 2.4 软件厂商



| | | |
|---|---|---|
| twitter | 1 | 20.00% |
| Tornado Authors | 1 | 20.00% |
| The jQuery Foundation. | 1 | 20.00% |
| The Open Group | 1 | 20.00% |
| VMS Software, Inc. | 1 | 20.00% |
| The PostgreSQL Global Development Group | 1 | 20.00% |
| Redis Labs | 1 | 20.00% |
| other | 1 | 20.00% |
| 共有：8 | | |

# 3．漏洞

| 名称（8） | 等级 | hostinfo | vulurl |
|---|---|---|---|
| 致远 OA A6 数据库敏感信息泄露 | 中危 | 47.251.44.45: 40636 | http://47.251.44.45:40636/yyoa/createMysql.jsp |

| | | | |
|---|---|---|---|
| JetBrains .idea project directory | 高危 | 47.251.44.45:40636 | http://47.251.44.45:40636/.idea/workspace.xml |
| D-Link DNS-320 login_mgr.cgi RCE (CVE-2019-16057) | 严重 | 47.251.44.45: 40700 | http://47.251.44.45:40700/cgi-bin/login_mgr.cgi?C1=ON&cmd=login&f_type=1&f_username=admin&port=80%7Cpwd%26id&pre_pwd=1&pwd=%20&ssl=1&ssl_port=1&username= |
| Atlassian Confluence 远程代码执行漏洞（CVE-2022-26134） | 中危 | 47.251.44.45:40700 | https://47.251.44.45:40700/%24%7B%28%23a%3D%40org.apache.commons.io.IOUtils%40toString%28%40java.lang.Runtime%40getRuntime%28%29.exec%28%22echo46r5vewrvwerwevrwevrwevrwevrwevrw%22%29.getInputStream%28%29%2C%22utf8%22%29%29.%28%40com.opensymphony.webwork.ServletA |

|  |  |  |  |
|---|---|---|---|
|  |  |  | ctionContext%40getResponse%28%29.setHeader%28%22XCmdResponse%22%2C%23a%29%29%7D/ |
| 用友 NC bsh.servlet.BshServlet 远程命令执行漏洞 | 严重 | http://47.251.44.45:40702 | http://47.251.44.45:40702/servlet/~ic/bsh.servlet.BshServlet |
| Git repository found | 严重 | http://47.251.44.45:40632 | http://47.251.44.45:40632/.git/config |
| DS_Store found | 严重 | http://47.251.44.45:40619 | http://47.251.44.45:40619/.DS_Store |
| Spring boot actuator unauthorized access | 严重 | http://47.251.44.45:40<br>629 | http://47.251.44.45:40629/actuator/ |

## 致远 OA A6 数据库敏感信息泄露 详情

中危 致远 OA A6 数据库敏感信息泄露

漏洞摘要

|  |  |
|---|---|
| 风险类型 | Other |

| | |
|---|---|
| 披露时间 | |
| URL | |
| 参考 | http://wiki.peiqi.tech |
| 标签 | 敏感信息泄露 |

描述

致远 OA A6 存在数据库敏感信息泄露，攻击者可以通过访问特定的 URL 获取数据库账户以及密码 MD5

## JetBrains .idea project directory 详情

高危 JetBrains .idea project directory

漏洞摘要

| | |
|---|---|
| 风险类型 | Other |
| 披露时间 | 2017-01-01 |
| URL | http://47.251.44.45:40636/.idea/workspace.xml |
| 参考 | https://www.acunetix.com/vulnerabilities/web/jetbrains-idea-project-directory/<br>https://github.com/lijiejie/idea_exploit |
| 标签 | infoleak<br>webvulscan |

描述

The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

漏洞危害

It allows malicious hackers to gather relevant information which can be used later in the attack lifecycle, in order to achieve more than they could if they didn’t get access to such information.

解决方案

Remove these files from production systems or restrict access to the .idea directory.

## D-Link DNS-320 login_mgr.cgi RCE (CVE-2019-16057) 详情

严重 D-Link DNS-320 login_mgr.cgi RCE (CVE-2019-16057)

漏洞摘要

| | |
|---|---|
| 风险类型 | Other |
| 披露时间 | 2021-06-02 |

| | |
|---|---|
| URL | http://47.251.44.45:40700/cgi-bin/login_mgr.cgi?C1=ON&cmd=login&f_type=1&f_username=admin&port=80%7Cpwd%26id&pre_pwd=1&pwd=%20&ssl=1&ssl_port=1&username= |
| 参考 | https://nvd.nist.gov/vuln/detail/CVE-2019-16057 |
| 标签 | RCE |

描述

The login_mgr.cgi script in D-Link DNS-320 through 2.05.B10 is vulnerable to remote command injection.

漏洞危害

The login_mgr.cgi script in D-Link DNS-320 through 2.05.B10 is vulnerable to remote command injection.

解决方案

Upgrade

## Atlassian Confluence 远程代码执行漏洞（CVE-2022-26134） 详情

严重 Atlassian Confluence 远程代码执行漏洞（CVE-2022-26134）

漏洞摘要

| | |
|---|---|
| 风险类型 | Other |
| 披露时间 | 2021-06-07 |
| URL | |

| | |
|---|---|
| 参考 | https://github.com/Nwqda/CVE-2022-26134 |
| 标签 | SQL 注入<br>代码执行 |

描述

2022 年 6 月 3 日，Atlassian Confluence 官方发布公告称 Confluence Server 和 Data Center 存在未授权远程代码执行漏洞，该漏洞由于 Confluence 将 URL 翻译成 namespace，导致攻击者可以在 URL 路径中构造 OGNL 表达式，造成表达式注入，从而远程代码执行。该漏洞被分配编号：CVE-2022-26134。

漏洞危害

该漏洞由于 Confluence 将 URL 翻译成 namespace，导致攻击者可以在 URL 路径中构造 OGNL 表达式造成表达式注入，从而远程代码执行。

解决方案

官方已经发布新版本，建议企业用户高优排查暴露在外网的服务并进行修复，安全版本包括：7.4.17、7.13.7、7.14.3、7.15.2、7.16.4、7.17.4、7.18.1

## 用友 NC bsh.servlet.BshServlet 远程命令执行漏洞 详情

### 严重 用友 NC bsh.servlet.BshServlet 远程命令执行漏洞

漏洞摘要

| | |
|---|---|
| 风险类型 | Other |
| 披露时间 | |
| URL | http://47.251.44.45:40628/servlet/~ic/bsh.servlet.BshServl |

| | |
|---|---|
| | et |
| 参考 | https://mp.weixin.qq.com/s/FvqC1I_G14AEQNztU0zn8A |
| 标签 | RCE |

描述

用友 NC bsh.servlet.BshServlet 存在远程命令执行漏洞，通过 BeanShell 执行行远程命令获取服务器权限

## Spring boot actuator unauthorized access 详情

严重 Spring boot actuator unauthorized access

漏洞摘要

| | |
|---|---|
| 风险类型 | Other |
| 披露时间 | |
| URL | http://47.251.44.45:40629/actuator/ |
| 参考 | https://gobies.org/ |
| 标签 | |

## DS_Store found 详情

严重 DS_Store found

漏洞摘要

| | |
|---|---|
| 风险类型 | Other |

| | |
|---|---|
| 披露时间 | 2017-01-01 |
| URL | http://47.251.44.45:40619/.DS_Store |
| 参考 | https://buildthis.com/ds_store-files-and-why-you-should-know-about-them/<br>https://github.com/lijiejie/ds_store_exp |
| 标签 | infoleak<br>webvulscan |

描述

A .DS_Store, short for Desktop Services Store, is an invisible file on the macOS operating system that gets automatically created anytime you look into a folder with ‘Finder.’ This file will then follow the folder everywhere it goes, including when archived, like in ‘ZIP’.

漏洞危害

This file stores custom attributes/metadata of its containing folder and the names of other files around it. Exposing this information could potentially allow hackers to act maliciously and let them see private files.

解决方案

The easiest way to prevent this problem from happening is to completely turn off the automatic creation of these files. For developers, you can use Git to solve this problem by .gitignore file.

## Git repository found 详情

### 严重 Git repository found

漏洞摘要

| | |
|---|---|
| 风险类型 | Other |
| 披露时间 | 2017-01-01 |
| URL | http://47.251.44.45:40632/.git/config |
| 参考 | https://www.acunetix.com/vulnerabilities/web/git-repository-found/<br>https://github.com/arthaud/git-dumper<br>https://github.com/lijiejie/GitHack |
| 标签 | infoleak<br>webvulscan |

描述

Subversion metadata directory (.svn) was found in this folder. An attacker can extract sensitive information by requesting the hidden metadata directory that popular version control tool Subversion creates. The metadata directories are used for development purposes to keep track of development changes to a set of source code before it is committed back to a central repository (and vice-versa). When code is rolled to a live server from a repository, it is supposed to be done as an export rather than as a local working copy, and hence this problem.

漏洞危害

It allows malicious hackers to gather relevant information which can be used later in the attack lifecycle, in order to achieve more than they could if they didn’ t get access to such information.

解决方案

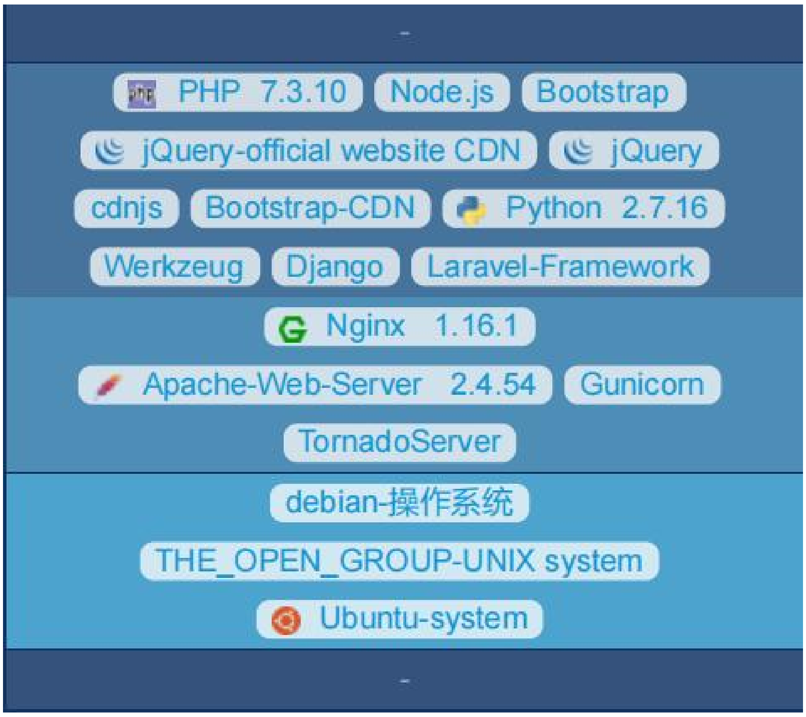
Remove these files from production systems or restrict access to the .idea directory.

## 4.资产

| IP（1） | 端口 | 协议 |
|---|---|---|
| 47.251.44.45 | 50000 | http |
| | 40703 | http |
| | 40702 | http |
| | 40700 | http |
| | 40636 | http |
| | 40635 | http |
| | 40634 | http |
| | 40633 | http |
| | 40632 | http |
| | 40631 | http |
| | 40630 | http |
| | 40629 | http |
| | 40628 | http |
| | 40627 | http |
| | 40626 | http |
| | 40625 | http |
| | 40624 | http |
| | 40623 | http |
| | 40622 | http |
| | 40621 | http |
| | 40620 | http |
| | 40619 | http |
| | 40618 | http |
| | 40617 | http |
| | 40616 | http |
| | 40615 | http |
| | 40614 | http |
| | 40613 | http |
| | 40612 | http |

|  |  |  |
|---|---|---|
|  | 40611 | http |
|  | 40610 | http |
|  | 40609 | http |
|  | 40608 | http |
|  | 40606 | http |
|  | 40604 | http |
|  | 40602 | http |

组件



-

PHP 7.3.10 Node.js Bootstrap

jQuery-official website CDN jQuery

cdnjs Bootstrap-CDN Python 2.7.16

Werkzeug Django Laravel-Framework

Nginx 1.16.1

Apache-Web-Server 2.4.54 Gunicorn

TornadoServer

debian-操作系统

THE_OPEN_GROUP-UNIX system

Ubuntu-system

-