



FIIT 2019

# 基于网络空间搜索引擎的通用漏洞挖掘

*heige@0x557*





## 关于我



FIT 2019

- 知道创宇CSO兼404实验室总监
- 0x557 、n0tr00t、80vul、ph4nt0m
- 微博/微信：hi\_heige
- twitter : @80vul





## 网络空间搜索引擎

IT 2019

- 2009年Shodan发布
- 2013年ZoomEye发布（项目启动2010年）
- 最新版本ZoomEye 2018
- 2015年Censys发布
- 2015 ~ 多家跟进





## 网络空间搜索引擎

FIIT 2019

- 网络空间测绘
- X计划、SHINE计划、藏宝图计划
- “看得清、防得住、可溯源”
- GPT-上帝模式的持续威胁 God Persistent Threat





## 网络空间漏洞评估

IT 2019

- › 漏洞影响评估是网络空间搜索引擎最常见核心应用
- › 常用于 通用组件的1Day/nDay评估
- › 漏洞组件指纹—>可能的影响范围—>抽样检测





- 漏洞挖掘的两个方向：
- 纵向：安全“红海”，安全对抗激烈的领域深耕细作
- 横向：寻找“蓝海”，漏洞随处可见！
- 网络空间中的漏洞挖掘更多的在于寻找“蓝海”
- 找到并能识别“蓝海”是关键





## 网络空间漏洞挖掘

IT 2019

- 对象：通用组件 —> 找漏洞先找通用组件
- 什么是通用组件？
  - 具有某些默认共同的特征元素的程序或者产品等
- 怎么找通用组件？(unknown消除)
  - 已知组件—>分析提取指纹—>打标（nmap等）
    - 被动、效率低、成本高、被硬件等局限





- 怎么找通用组件？
  - 聚类—>识别—>提取指纹—>打标
- 聚类
  - AI算法聚类：全面、整体、多维，局限于平台方
  - 手工聚类：具体、细分，利用搜索引擎查询语法







怎么手工聚类？

选取目标协议：如http

通用组件丰富

Banner数据结构完整，可读性强。





## 聚类

FIIT 2019

- 从http协议看通用组件的“通用”元素
  - http头：如通用的Server、独特的http头、默认的Location/Set-Cookie/Content-Length等的值
  - html body：如特有的title、产品开发相关的特有关键词等。
- 默认安装的“通用”元素：如端口



# 聚类

FIIT 2019

The screenshot shows a ZoomEye search interface. The search query is "Server: Jetty", which is circled in red. The results are divided into two main sections: "DEVICE" and "PORT".

**DEVICE**

Unknown	1,358,221
load balancer	2

**PORT**

8080	327,392
5555	158,400
80	127,735
443	94,662
8081	66,358
50075	42,276
7070	36,767
4040	34,870
8443	33,968
50070	29,615

A large red circle highlights the "PORT" table, with a handwritten "2" next to it. Another red circle highlights the search query "Server: Jetty".

**Search Results Details:**

- 71.95.50.180** (United States, Riverside): HTTP/1.1 200 OK, Content-Type: text/html, Content-Length: 2533, Last-Modified: Wed, 30 Aug 2017 01:10:50 GMT, Server: Jetty(8.y.z-SNAPSHOT). Path: 8123/http.
- 71.202.74.132** (United States, San Jose): HTTP/1.1 200 OK, Content-Type: text/html, Content-Length: 2757, Last-Modified: Thu, 04 Oct 2018 05:50:14 GMT, Server: Jetty(8.y.z-SNAPSHOT). Path: 8123/http.



"Server: Jetty+port:"4040"

IT 2019

The screenshot shows a network log with three entries, each representing an HTTP 302 Found response. Each entry is highlighted with a red box around the response headers.

IP Address	Response Headers
119.17.132.131	<pre>HTTP/1.1 302 Found Expires: Thu, 01 Jan 1970 00:00:00 GMT Set-Cookie: JSESSIONID=sqJ5xiabljd;Path=/ Location: http://192.168.1.2:4040/login.view;sessionId=sqJ5xiabl Content-Length: 0 Server: Jetty(6.1.x)</pre>
119.173.246.20	<pre>HTTP/1.1 302 Found Expires: Thu, 01 Jan 1970 00:00:00 GMT Set-Cookie: JSESSIONID=zw8bqr2ypw8;Path=/ Location: http://192.168.0.5:4040/login.view;sessionId=zw8bqr2yp Content-Length: 0 Server: Jetty(6.1.x)</pre>
119.81.212.152	<pre>HTTP/1.1 302 Found Location: http://119.81.212.152:4040/jobse/ Content-Length: 0 Server: Jetty(8.y.a-SNAPSHOT)</pre>



## 关键词+回归测试

2019

- Location: `http://192.168.1.2:4040/login.view;jsessionid=zgu35xiabljd?`
- <https://www.zoomeye.org/searchResult?q=%22login.view%3Bjsessionid%22>
- 注意最后我们的指纹与开始选用通用元素如Server头/端口等无关。
- 通用元素可能是默认元素，可能是最多的，但不是最全的





https://www.zoomeye.org/searchResult?q="login.view%3BjsessionId"&t=all

ZoomEy

Home

Explore

Developer

Topics

Business

Shared

Privatization

"login.view;jsessionId"

184.59.221.169

cpe-184-59-221-169.new.res.rtr.com

4040/http

United States, Green Bay

2018-11-22 12:28

HTTP/1.1 302 Found

Expires: Thu, 01 Jan 1970 00:00:00 GMT

Set-Cookie: JSESSIONID=fzygdpak26wr;Path=/  
Location: http://192.168.1.153:4040/login.view;jsessionId=fzygdpak;

Content-Length: 0

Server: Jetty(6.1.x)

184.103.105.151

United States, Phoenix

2018-11-22 12:28

HTTP/1.1 302 Found

Expires: Thu, 01 Jan 1970 00:00:00 GMT

Set-Cookie: JSESSIONID=gzpkgupnlrdd;Path=/  
Location: http://192.168.1.2:4040/login.view;jsessionId=gzpkgupnlr

Content-Length: 0

Server: Jetty(6.1.x)

PORT

4040	25,808
80	2,856
8080	2,057
443	1,220
4443	525
8443	412
81	323
8081	314
8000	118
82	90

IT 2019





识别

IFT 2019

The screenshot shows the Subsonic website interface. At the top, there is a navigation menu with links for Home, Premium, News, Songs, and Artists. The main header features a large crowd of people with their hands raised, and the Subsonic logo with the tagline "Your complete, personal media streamer". Below the header, there is a URL bar showing "91.160.234.77:49153/login.view;jsessionid=zkjgzo5uplf?". The main content area contains the Subsonic logo and a login form with the following fields:

- Utilisateur:
- Mot de passe:
- Entrer button
- Se souvenir de moi
- Mot de passe oublié link





FIIT 2019

# 漏洞挖掘







## 从BrickerBot说起

FIIT 2019

- › Mirai —> BrickerBot
  - › Ddos: Mirai抓鸡, BrickerBot杀鸡
  - › 源于Dr Cyborkian a.k.a. janit0r发起的项目“Internet Chemotherapy”
  - › <https://archive.is/PQAnU#selection-13.5156-13.5200>
  - › 更像是一场“社会实践”！





```
Internet
Chemotherapy

PART 9
Bricking Basics and DIY

by Dr Cyborkian a.k.a. janit0r - conditioner of 'terminally ill' devices

previous parts can be found at least here:
original (Project Introduction):
https://0x00sec.org/t/Internet-Chemotherapy/4964

part 2 (ISPs: Lessons from the Rogers Hi-Speed Internet incident):
http://deposedihrn3jtw.enion.to/show.php?ed5=ee7136ac407a587fa88388fbcb6d788 (Clearnet)
http://deposedihrn3jtw.enion/show.php?ed5=ee7136ac48fa9fba88388fbcb6d788 (Tar)

part 3 (ISPs: The baffling case of @otify/Keycom's mismanagement):
http://deposedihrn3jtw.enion.to/show.php?ed5=7e7bfe486315f128d8ed325ff6b7678b (Clearnet)
http://deposedihrn3jtw.enion/show.php?ed5=7e7bfe486315f128d8ed325ff6b7678b (Tar)

part 4 (ISPs: The dirty case of Telkom South Africa):
http://deposedihrn3jtw.enion.to/show.php?ed5=11838bc79a079f5b7bc33bcca84641f6 (Clearnet)
http://deposedihrn3jtw.enion/show.php?ed5=11838bc79a079f5b7bc33bcca84641f6 (Tar)

part 5 (The IoT Battlefield: Device Stability):
http://deposedihrn3jtw.enion.to/show.php?ed5=8ca2bcadeb75137725557a24848d3c17 (Clearnet)
http://deposedihrn3jtw.enion/show.php?ed5=8ca2bcadeb75137725557a24848d3c17 (Tar)

part 6 (The IoT Battlefield: Mitigation Methods):
http://deposedihrn3jtw.enion.to/show.php?ed5=2c822a998ff22d56f3b9eb89ed722c3f (Clearnet)
http://deposedihrn3jtw.enion/show.php?ed5=2c822a998ff22d56f3b9eb89ed722c3f (Tar)

part 7 (The IoT Battlefield: Default Passwords):
http://deposedihrn3jtw.enion.to/show.php?ed5=a4232ae8f56834348323ab4483187abb (Clearnet)
http://deposedihrn3jtw.enion/show.php?ed5=a4232ae8f56834348323ab4483187abb (Tar)

part 8 (The IoT Battlefield: The where and why):
http://deposedihrn3jtw.enion.to/show.php?ed5=2a7d5afa2731381a6ead86da3805e5d (Clearnet)
http://deposedihrn3jtw.enion/show.php?ed5=2a7d5afa2731381a6ead86da3805e5d (Tar)
```





# VTECH IP Camera/NVR/DVR Devices



Below is a table of the top 50 countries (counting unique IP:port:login triplets):

#	Country	Count	Ratio	Most Common Login
1	Sri Lanka	12278	(12.8%)	admin/admin (99%)
2	Mexico	61406	(13.4%)	admin/admin (57%)
3	Indonesia	60425	(13.2%)	admin/admin (71%)
4	Thailand	50834	(12.3%)	admin/admin (61%)
5	Vietnam	43822	(9.6%)	admin/admin (71%)
6	Malaysia	32966	(7.2%)	admin/admin (78%)
7	Italy	7846	(1.7%)	admin/admin (56%)
8	Germany	7266	(1.7%)	admin/admin (39%)
9	Argentina	6987	(1.5%)	admin/admin (46%)
10	Singapore	6666	(1.5%)	admin/admin (74%)
11	United States	6066	(1.3%)	admin/admin (66%)
12	Hong Kong	5884	(1.3%)	admin/admin (63%)
13	The Philippines	5246	(1.2%)	admin/admin (67%)
14	Great Britain	4756	(1.2%)	admin/admin (67%)

Finally, let's move on to the top 100 overall common logins for the vulnerable Avtech units (counting unique IP:port:login triplets):

#	Login	Count	Ratio	Top Country for Login
1	admin/admin	31126	(68.2%)	Sri Lanka (53%)
2	admin/8888	3438	(8.8%)	Mexico (16%)
3	admin/1234	1401	(3.3%)	Thailand (52%)
4	admin/123456	1199	(3.3%)	Vietnam (52%)
5	admin/12345	1031	(3.2%)	Thailand (52%)
6	admin/mon9n	1004	(3.2%)	Thailand (100%)
7	admin/admin1	863	(3.2%)	Thailand (57%)
8	admin/admin123	707	(3.2%)	Indonesia (37%)
9	admin/system*	577	(3.1%)	Mexico (100%)
10	admin/1111	525	(3.1%)	Thailand (86%)





# Wificam

IT 2019

#	Country	Count	Ratio	Most Common Login
1	China	63702	(22.9%)	admin/ (61%)
2	Vietnam	60020	(21.5%)	admin/admin (53%)
3	United States	20657	(7.4%)	admin/ (34%)
4	Thailand	16064	(5.8%)	admin/ (58%)
5	Mexico	11832	(4.2%)	admin/ (73%)
6	Italy	10492	(3.8%)	admin/888888 (36%)
7	Great Britain	9912	(3.6%)	admin/ (38%)
8	Malaysia	8738	(3.1%)	admin/ (53%)
9	Turkey	5797	(2.1%)	admin/admin (50%)
10	Russia	4988	(1.8%)	admin/ (40%)

#	Login	Count	Ratio	Top Country for Login
1	admin/	112221	(40.3%)	China (35%)
2	admin/admin	62515	(22.4%)	Vietnam (51%)
3	admin/888888	4605	(1.7%)	Italy (83%)
4	admin/123456	2431	(0.9%)	China (49%)
5	admin/none	1729	(0.6%)	Thailand (18%)
6	admin/admin99	1369	(0.5%)	Italy (33%)
7	admin/1234	846	(0.3%)	Thailand (27%)
8	admin/admin123	696	(0.2%)	Vietnam (76%)
9	admin/12345	641	(0.2%)	Vietnam (46%)
10	admin/12345678	605	(0.2%)	Vietnam (41%)



#	Country	Count	Ratio	Most Common Login
1	India	664183	(35.2%)	888888/888888 (51%)
2	Vietnam	197736	(10.5%)	888888/888888 (61%)
3	Brazil	129303	(6.9%)	888888/888888 (39%)
4	United States	82868	(4.4%)	888888/888888 (30%)
5	Mexico	52407	(2.8%)	888888/888888 (69%)
6	Sri Lanka	46742	(2.5%)	888888/ntc260 (38%)
7	Thailand	42884	(2.3%)	888888/888888 (74%)
8	Chile	33402	(1.8%)	888888/888888 (68%)
9	Poland	32926	(1.7%)	888888/888888 (51%)
10	Spain	31513	(1.7%)	888888/888888 (55%)

#	Login	Count	Ratio	Top Country for Login
1	888888/888888	451240	(51.9%)	India (23%)
2	888888/	55805	(6.4%)	India (71%)
3	admin/admin	33290	(3.8%)	Brazil (42%)
4	888888/ntc260	11789	(1.4%)	Sri Lanka (100%)
5	admin/vista1	7906	(0.9%)	Sri Lanka (100%)
6	888888/123456	6751	(0.8%)	India (62%)
7	admin/1234	5615	(0.6%)	Canada (31%)
8	admin/123456	5543	(0.6%)	United States (36%)
9	default/tluaFed	5179	(0.6%)	India (31%)
10	888888/admin	2552	(0.3%)	India (69%)



# XiongMai

IT 2019

#	Country	Count	Ratio	Most Common Login
1	Vietnam	1272423	(24.5%)	admin/ (55%)
2	Uruguay	576040	(11.1%)	admin/ (29%)
3	India	539351	(10.4%)	admin/ (61%)
4	Brazil	508820	(9.8%)	admin/ (50%)
5	Thailand	265904	(5.1%)	admin/ (70%)
6	Turkey	222044	(4.3%)	admin/ (52%)
7	Sri Lanka	194218	(3.7%)	admin/ (33%)
8	Morocco	144932	(2.8%)	admin/ (60%)
9	Malaysia	123773	(2.4%)	admin/ (60%)
10	China	120292	(2.3%)	admin/ (85%)

#	Login	Count	Ratio	Top Country for Login
1	admin/	2678930	(51.7%)	Vietnam (26%)
2	admin/123456	202777	(3.9%)	Vietnam (28%)
3	admin/admin	150098	(2.9%)	India (51%)
4	admin/siera	124910	(2.4%)	Uruguay (97%)
5	admin/123abc456	38534	(0.7%)	Vietnam (99%)
6	admin/1234	38258	(0.7%)	Uruguay (15%)
7	admin/12345	34013	(0.7%)	India (16%)
8	admin/888888	25261	(0.5%)	Vietnam (33%)
9	admin/686868	14812	(0.3%)	Vietnam (99%)
10	admin/1	12074	(0.2%)	Brazil (57%)





思考

FIIT 2019

- › 当“悲观主义”拥有了“上帝之眼” ...
- › 研究技术的意义何在？
- › 看清—>通透—>积极应对





## 漏洞类型：默认口令

IT 2019

- 通用组件—>默认共性—>默认安全风险
- “Secure by Default”原则 [https://en.wikipedia.org/wiki/Secure\\_by\\_default](https://en.wikipedia.org/wiki/Secure_by_default)
- 漏洞类型：
  - 默认安装用户名及密码
  - 预留硬编码用户名及密码（后门）







## 默认用户名及密码

FIIT 2019

- 方法一：聚类识别—>官方安装说明（用户名/密码）—>抽样检测
  - 可能有多组默认用户及密码
  - 默认密码可能为某标示最后几位数 如mac地址/数字sn等





https://www.zoomeye.org/searchResult?q="Server%3A%20Agranat-EmWeb/R5\_2\_4"

知道创宇 | ZoomEy Home Explore Developer Topics Business Shared Privatization

"Server: Agranat-EmWeb/R5\_2\_4"

Result Report Maps Vulnerability tokenizer share download

About 6,472 results 0.130 seconds

"Server: Agranat-EmWeb/R5\_2\_4" X

162.211.53.134	HTTP/1.1 301 Moved Permanently Date: Sat, 24 Nov 2018 13:41:45 GMT Server: Agranat-EmWeb/R5_2_4 Location: http://web/content/index.html Content-Type: text/html Content-Length: 98
United States, New York	
2018-11-24 16:05	

96.30.105.246	HTTP/1.1 301 Moved Permanently Date: Wed, 02 Feb 2000 16:08:17 GMT Server: Agranat-EmWeb/R5_2_4 Location: http://ç8Us'²ÄÖü">VoA²ÄFÜ:Kjp_Ä/web/content/index.htm Content-Type: text/html Content-Length: 130
Thailand, Bangkok	
2018-11-24 12:29	

SEARCH TYPE

Devices	6,454
Websites	18

YEAR

2018	2,515
2017	1,845
2016	1,008
2015	981
2014	123

COUNTRY

United States	2,297
---------------	-------

FIIT 2019





alcatel-lucent webview default password



All Images News Videos Shopping More Settings Tools

About 12,300 results (0.60 seconds)

### Alcatel-Lucent OmniSwitch 6250 Switch Default Admin Credentials ...

<https://dariusfreamon.wordpress.com/.../alcatel-lucent-omniswitch-6250-switch-defaul...>

Feb 28, 2016 - Alcatel-Lucent OmniSwitch 6250 Switch can be managed via telnet console or HTTP via a utility they call WebView. The switch creates a ...



Search. Home Alcatel. Alcatel logo. Alcatel devices. PBX systems, mobile phones, various communication hardware <http://www.alcatel-lucent.com/> ...

### [PDF] OmniSwitch 6900 Getting Started Guide - Alcadis Support

[support.alcadis.nl/\\_jget\\_file?...Alcatel-Lucent%252FOmniSwitch%252FOS6900%25...](support.alcadis.nl/_jget_file?...Alcatel-Lucent%252FOmniSwitch%252FOS6900%25...)

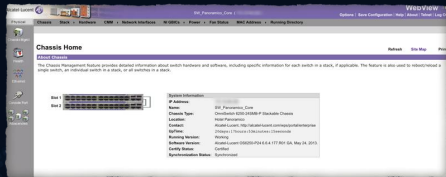
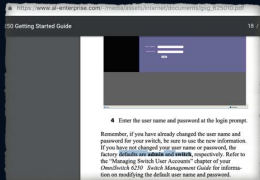
Aug 4, 2011 - Changing the Login Password . ... The Alcatel-Lucent OmniSwitch 6900 (OS6900) is a high-capacity ... default values, examples, usage guidelines, and. CLI-to-MIB variable ... system configuration, SNMP, and WebView.

IT 2019





FIIT 2019





# 默认用户名及密码



方法二：设备/组件默认密码—>提取指纹—>搜索

default password list

Order by character: ABCDEFGHIJKLMNOPQRSTUVWXYZ0-9

Displaying 1812 passwords of total 1812 entries.

Manufacturer	Product	Revision	Protocol	User	Password
COM			Telnet	adm	(none)
COM			Telnet	security	security
COM			Telnet	read	spinet
COM			Telnet	write	spinet
COM			Telnet	admin	spinet
COM			Telnet	manager	manager
COM			Telnet	monitor	monitor
COM			Telnet	security	security
COM	3Com SuperStack 3 Switch 13000H		Multi	n/a	(none)
COM	AirConnect Access Point	01.50-01	Multi	n/a	(none)
COM	Bozon router simulator	3.65	HTTP	admin	admin
COM	catplox	7900	Telnet	admin	admin
COM	CallPlex	7900	Telnet	tech	tech
COM	CallPlex		HTTP	admin	spinet
COM	CoreBuilder	7900/1000/2100/2500	Telnet	debug	spinet
COM	CoreBuilder	7900/1000/2100/2500	Telnet	tech	tech
COM	HiWayMTC	v4.1.x	Telnet	adm	(none)
COM	hub		Multi	n/a	(none)
COM	LANplex	2500	Telnet	tech	tech
COM	LANplex	2500	Telnet	tech	(none)
COM	LANplex	2500	Telnet	debug	spinet
COM	LinkBuilder		Telnet	n/a	(none)
COM	LinkSwitch	2800/2700	Telnet	tech	tech
COM	NetBuilder		SNMP	(none)	admin
COM	NetBuilder		SNMP		ANYCOM
COM	NetBuilder		SNMP		LSM
COM	Office Connect 100N Routers	540	Telnet	n/a	PASSVORO
COM	OfficeConnect 812 ADSL router		Multi	admin@	admin@
COM	router		Multi	n/a	(none)
COM	super stack 2 switch		Multi	manager	manager
COM	super stack 2E		Console	n/a	(none)
COM	SuperStack II	1100/1300	Console	3com3cu	R3000
COM	SuperStack II Switch	2700	Telnet	tech	tech
COM	SuperStack II Switch	2200	Telnet	debug	spinet
COM	Wireless 11g Pivotal Router	3CWR0100-T2	Multi	none	admin
COM	Wireless AP	AMP	Multi	admin	comconcom
COM	WOL-6115 etc.		SNMP	vollton	vollton





## 硬编码用户/密码后门

IFT 2019

### Cisco IOS XE Software Static Credential Vulnerability

Critical

<b>Advisory ID:</b>	cisco-sa-20180328-xesc	CVE-2018-0150	<a href="#">Download CVRF</a>
<b>First Published:</b>	2018 March 28 16:00 GMT	CWE-798	<a href="#">Download PDF</a>
<b>Last Updated:</b>	2018 September 19 16:00 GMT		<a href="#">Email</a>
<b>Version 2.0:</b>	Final		
<b>Workarounds:</b>	Yes		
<b>Cisco Bug IDs:</b>	<a href="#">CSCve76719</a>		
	<a href="#">CSCve89880</a>		
<b>CVSS Score:</b>	Base 9.8		

#### Summary

A vulnerability in Cisco IOS XE Software could allow an unauthenticated, remote attacker to log in to a device running an affected release of Cisco IOS XE Software with the default username and password that are used at initial boot.

The vulnerability is due to an undocumented user account with privilege level 15 that has a default username and password. An attacker could exploit this vulnerability by using this account to remotely connect to an affected device. A successful exploit could allow the attacker to log in to the device with privilege level 15 access.





## 漏洞类型：认证缺省

IT 2019

- MongoDB、Redis、Hadoop和CouchDB勒索及挖矿
- 流行的NOSQL数据、服务端JS/Go/JAVA类框架、工控iot项目等
- 一般方法：聚类识别访问就可以确认





## 漏洞类型：认证缺省

IT 2019

- 搜索引擎的方法：
  - http协议：可以通过http状态码识别 200 vs 401





Two screenshots of a web browser's developer console showing HTTP error messages. The left screenshot shows a '404 Not Found' error and a '401 Unauthorized' error. The right screenshot shows a '400 Bad Request' error. Red boxes highlight the error codes and status codes.

### Rosin Lower

Option	Description
<a href="#">View Data</a>	Display a list showing available data pages.
<a href="#">View Logs</a>	Download files from the data logger.
<a href="#">Remote View</a>	Display a view of the HMI's display and keyboard.

Powered by [Red Lion](#).

IT 2019



## 漏洞类型：认证缺省

IT 2019

搜索引擎的方法：

telnet协议：通过 - 运算找没有认证的目标





Search results for 'Sollae Systems' showing IP addresses and hostnames. A red box highlights the IP address 128.170.100.12 and the hostname 'panweds'.

Search results for 'Sollae Systems' showing IP addresses and hostnames. A red box highlights the '-password' field in the search criteria.

```
form git:(master) telnet 128.170.100.12
Trying 128.170.100.12:241...
Connected to 128.170.100.12.
Escape character is '^]'.
SE-M53 Management Console v1.0G Sollae Systems
sh>st net
Proto Name Local Address Peer Address Sendq State
-----
CP tty 128.170.100.241(23) 128.170.100.7(32990) 219 ESTABLISHED
CP com1 128.170.100.241(59032) 128.170.100.65(2000) 0 ESTABLISHED
sh>st uptime
17:55:10.26 up 31 days
sh>
```





# 敏感信息泄露漏洞

IT 2019


从 CVE-2018-12634 说起

CVE-ID	
<b>CVE-2018-12634</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
CirCarLife Scada before 4.3 allows remote attackers to obtain sensitive information via a direct request for the html/log or services/system/info.html URI.	
References	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"><li>• EXPLOIT-DB:45384</li><li>• URL:<a href="https://www.exploit-db.com/exploits/45384/">https://www.exploit-db.com/exploits/45384/</a></li><li>• MISC:<a href="https://www.seebug.org/vuldb/ssvid-97353">https://www.seebug.org/vuldb/ssvid-97353</a></li><li>• MISC:<a href="https://github.com/SadFud/Exploits/tree/master/Real%20World/Suites/cir-pwn-life">https://github.com/SadFud/Exploits/tree/master/Real%20World/Suites/cir-pwn-life</a></li></ul>	





→ ↻ 不安全 | http://html/upgrade.html



**Compromiso con la innovación**  
*Commitment to innovation*

The upgrade process will take approximately 1 minute. When it's done, the device will reboot automatically.  
**Don't power down the device once *upgrade* is clicked.**

选择文件 未选择任何文件

Upgrade



```
➤ curl -k https://www.mobilis.com/mbis/loy-igmp-4xw
% Total % Received % Xferd Average Speed Time Time Time Current
         Dload Upload Total Spent Left Speed
  0 154k  0 13312  0  0 4506  0 0:00:35 0:00:02 0:00:33 4504(standard input)-72-May 9 01:23:38 eds
opcomp # (from /etc/ppp/peers/gprs)
standard input)-73-May 9 01:23:38 eds daemon.info pppd[21460]: lcp-echo-failure 3 # (from /etc/ppp/peer
standard input)-74-May 9 01:23:38 eds daemon.info pppd[21460]: lcp-echo-interval 50 # (from /etc/ppp/peer
standard input)-75-May 9 01:23:38 eds daemon.info pppd[21460]: show-password # (from /etc/ppp/peers/gprs)
standard input)-76-May 9 01:23:38 eds daemon.info pppd[21460]: novj # (from /etc/ppp/peers/gprs)
standard input)-77-May 9 01:23:38 eds daemon.info pppd[21460]: novjccomp # (from /etc/ppp/peers/gprs)
standard input)-78-May 9 01:23:38 eds daemon.info pppd[21460]: ipcp-accept-local # (from /etc/ppp/peer

standard input)-96-May 9 01:23:40 eds daemon.debug pppd[21460]: rcvd [LCP ConfReq id=0x3 <asyncmap 0x0> <msr 1500>
standard input)-97-May 9 01:23:40 eds daemon.debug pppd[21460]: sent [LCP ConfAck id=0x3 <asyncmap 0x0> <msr 1500>
standard input)-98-May 9 01:23:40 eds daemon.debug pppd[21460]: sent [LCP EchoReq id=0x0 magic=0x29d0f12b]
standard input)-99-May 9 01:23:40 eds daemon.debug pppd[21460]: sent [PAP AuthReq id=0x1 user="1234" password="1234"]
standard input)-100-May 9 01:23:40 eds daemon.debug pppd[21460]: rcvd [LCP EchoRep id=0x0 magic=0x543]
standard input)-101-May 9 01:23:40 eds daemon.debug pppd[21460]: rcvd [PAP AuthAck id=0x1 "Greetings!!"]
standard input)-102-May 9 01:23:40 eds daemon.info pppd[21460]: Remote message: Greetings!!
  11 154k  11 40300  0  0 10000  0 0:00:15 0:00:04 0:00:11 10000
```





## 敏感信息泄露漏洞

IT 2019

- 提取URL
  - 在匿名能访问的页面里爬取 (如 CVE-2018-12634)
  - 使用默认密码/弱密码登录后爬取 (如 CVE-2018-12594)
- 访问URL
  - 通过跟提取URL的目标IP与访问URL目标IP分开
  - 注意去掉认证Cookie等信息进行测试
- 可自动化实现
- 同样适用其他漏洞类型XSS/SQLi/RCE等, 但不适合Dos/溢出等漏洞





## “组件基因”与漏洞

IFT 2019

- 组件基因与软件基因
  - 组件基因：网路空间里的组件指纹
  - 软件基因：常常用于恶意软件溯源
- 通用基础组件：
  - 不通的品牌设备可能使用同一基础组件
  - 那么同一基础组件的漏洞会影响多个不通品牌的设备







# 抓住“新代码”的影子

——基于 GoAhead 系列网络摄像头多个漏洞分析



知道创宇 404 实验室

## 1. 更新情况

版本	时间	备注
第一版	2017-05-19	抓住“新代码”的影子——基于 GoAhead 系列网络摄像头多个漏洞分析

## 2. 漏洞背景

GoAhead 作为世界上最受欢迎的嵌入式 Web 服务器被部署在物联网设备中，是各种嵌入式设备与应用的理想选择。当然，各厂商也会根据不同产品需求对其进行一定程度的二次开发。

2017 年 3 月 7 日，Seebug 漏洞平台收录了一篇基于 GoAhead 系列摄像头的多个漏洞，作者名为 Pierre Kim 在博客上发表的一篇文章，**披露了高达于 3750 多个摄像头型号的几个通用型漏洞**，其在文章中将其中的一个验证绕过漏洞以及为 GoAhead 服务器的漏洞。据事后证明，该漏洞却是由厂商二次开发 GoAhead 服务器产生的。于此同时，Pierre Kim 将其中两个漏洞结合使用，成功获取了摄像头的最高权限。

## 3. 漏洞分析

当我们开始着手分析这些漏洞时发现 GoAhead 官方源码不存在该漏洞，解开的更新固件无法找到对应程序，一系列困难接踵而至。好在根据该漏洞特殊变量名称 loginse 和 loginpw，我们在 github 上找到一个上个月还在修改的[门控项目](#)，顺着这个“新代码”的影子，我们不仅分析出了漏洞原理，还通过分析结果找到了漏洞新的利用方式。

由于该项目依赖的一些外部环境导致无法正常编译，我们仅仅通过静态代码分析得出结论，因此难免有疏漏，如有错误，欢迎指正。:)

1 验证绕过导致信息（登录凭据）泄露漏洞



## “组件基因”与漏洞

FIIT 2019

- › OEM产业链
  - › OEM系列产品必然带入同样基因
  - › 基因存在漏洞必然影响多家OEM系列产品





## 大华摄像头敏感信息泄露漏洞事件分析



知道创宇404实验室

2017-03-21

我们注意到“9b9171749866e18f2d2b479866660e”值的品牌摄像头数据量多达19704，远远超过了其他4组的数据。这些设备的型号列表如下：



没有看到明确的“品牌”属性，于是我们通过谷歌搜索找到如下网页：<http://www.worldsystem.com/blog/technical-questions/configuring-ntp-maxcampro.html> 关联到一个叫“maxcampro”的品牌摄像头。

根据以上分析，我们大致的推测4组不同的tevcam-xxx文件的品牌的摄像头设备基于大华设备品牌列表，具体发布如下<https://github.com>：

品牌	厂商	型号	URL	数量
Maxcampro	大华	9b9171749866e18f2d2b479866660e	http://www.worldsystem.com/blog/technical-questions/configuring-ntp-maxcampro.html	19704
Maxcampro	大华	9b9171749866e18f2d2b479866660e	http://www.worldsystem.com/blog/technical-questions/configuring-ntp-maxcampro.html	19704
Maxcampro	大华	9b9171749866e18f2d2b479866660e	http://www.worldsystem.com/blog/technical-questions/configuring-ntp-maxcampro.html	19704
Maxcampro	大华	9b9171749866e18f2d2b479866660e	http://www.worldsystem.com/blog/technical-questions/configuring-ntp-maxcampro.html	19704
Maxcampro	大华	9b9171749866e18f2d2b479866660e	http://www.worldsystem.com/blog/technical-questions/configuring-ntp-maxcampro.html	19704

针对数量最多的型号“maxcampro”的品牌摄像头地址进行了全球地区分布统计：



## 一个非典型案例

CTF 2019

The screenshot shows a web browser displaying a vulnerability entry on the Seebug website. The URL is <https://www.seebug.org/vuldb/ssvid-97674>. The page title is "Link-Net LW-N605R 12.20.2.1486 - Remote Code Execution (CVE-2018-16752)". The entry details include:

- SSV ID: SSV-97674
- Find Time: Unknown
- Submit Time: 2018-11-13
- Level:
- Category: 代码执行
- Component:
- Author: Nassim Asir
- Submitter: Knowsec
- CVE-ID: CVE-2018-16752
- CNVD-ID: [Add](#)
- CWE-ID: [Add](#)
- ZoomEye Dark: [Add](#)

On the right side, there is a list of users who have interacted with the entry:

- None 参与了评论
- None 参与了评论
- anonymous 参与了评论

At the bottom, there is a "Source" section with the URL: <https://www.exploit-db.com/exploits/45351/>. A "Timeline" section is also visible, showing the entry was submitted by Nassim Asir on 2018-11-13.



```
async def do_some_work(self, url, result_queue):
    headers = {'User-Agent': 'Mozilla/4.0 (compatible; MSIE 5.5; Windows NT)'}
    target_res = {'url': url, 'account': {}}
    try:
        async with aiohttp.ClientSession() as session:
            async with session.get(url, headers=headers, timeout=5, verify_ssl=False) as resp:
                if resp.status != 401 or resp.headers['Server'] != 'GoAhead-Webs':
                    return False
            for k, v in {'admin': 'admin'}.items():
                headers['Authorization'] = 'Basic {}'.format(base64.b64encode((k + ':' + v).encode(encoding='utf-8')).decode())
                async with session.get('%s/gofarm/sysTools' % url, headers=headers, timeout=5, verify_ssl=False) as resp1:
                    if resp1.status == 200:
                        target_res['account'][k] = v
    except Exception as e:
        if self.options['verbose']:
            print('{} {}'.format(url, str(e)))
```

抽样测试 1/1000

成功的设备为：

HiPER 4220G - qv4220Gv2.2.0-140912

<http://www.utt.com.cn/productdetail.php?modelid=163>





# CVE-2018-19243



```
Desktop proxychains4 curl -i -u "admin:admin" http://127.0.0.1/goform/formExportSettings
proxychains] config file found: /usr/local/etc/proxychains.conf
proxychains] preloading /usr/local/Cellar/proxychains-ng/4.13/lib/libproxychains4.dylib
proxychains] DLL init: proxychains-ng 4.13
proxychains] Strict chain ... 127.0.0.1:8899 ... 127.0.0.1:8081 ... OK
HTTP/1.1 200 OK
pragma: no-cache
cache-control: no-cache
content-type: application/octet-stream;charset=gb2312
content-Transfer-Encoding: binary
content-Disposition: attachment; filename="config_201811122303.xml";
content-Length: 2209

<?xml version="1.0" encoding="gb2312"?><config><sysConf /><interface><case
name="0"><active>Yes</active><ethernet><static><ip>192.168.88.1</ip></static><pppoe /></ethernet></case><case
name="1"><active>Yes</active><ethernet><connMode>PPPOE</connMode><static /><pppoe><user>073...319</user><passwd>a123456</passwd><mtu>1480</mtu></pppoe></ethernet><isp>10000</is
</interface>
```





## 安全启示

FIIT 2019

- 看得清，才可能防得住！
- 安全在对抗中进步！

