Report Generated:
Mon Feb 22 2021 12:12:16 GMT+1000 (Australian Eastern Standard Time)

Create by Shannon Setter

BEWEAR

IP	Hostname	Vendor	MAC	OSCPE	OSCVE	OSEx	Ports
192.168.0.1	dlinkrouter	D-Link International	28:3B:82:64:37:B7	cpe:/o:linux:linux_kernel:2.6	66	26	7
192.168.0.108	osmc	Raspberry Pi Foundation	B8:27:EB:C3:5D:6E	cpe:/o:linux:linux_kernel:3	0	0	3
192.168.0.131	Chromecast-Ultra	Salcomp (Shenzhen)	44:09:B8:0F:8D:6C	cpe:/o:linux:linux_kernel:3	0	0	5
192.168.0.208				cpe:/o:microsoft:windows	73	8	9

192.168.0.1 || 28:3B:82:64:37:B7			
Port	**Name**	**Product**	**Cpe**
53	domain	dnsmasq	cpe:/a:thekelleys:dnsmasq:2.78
80	http	lighttpd	cpe:/a:lighttpd:lighttpd:1.4.20
2601	quagga	Quagga routing software	cpe:/a:quagga:quagga:1.1.1
2602	quagga	Quagga routing software	cpe:/a:quagga:quagga:1.1.1
8008			
8888	upnp	MiniUPnP	cpe:/a:miniupnp_project:miniupnpd:1.6
49152	http	lighttpd	cpe:/a:lighttpd:lighttpd:1.4.20

192.168.0.108 || B8:27:EB:C3:5D:6E			
Port	**Name**	**Product**	**Cpe**
22	ssh	OpenSSH	cpe:/a:openbsd:openssh:7.4p1
80	http		cpe:/a:jeremy_graham:chorus:2
111			

192.168.0.131 || 44:09:B8:0F:8D:6C			
Port	**Name**	**Product**	**Cpe**
8008			
8009			
8443			
9000			
10001			

192.168.0.208 ||			
Port	**Name**	**Product**	**Cpe**
80	http	Apache httpd	cpe:/a:apache:http_server:2.4.41
135	msrpc	Microsoft Windows RPC	cpe:/o:microsoft:windows
139	netbios-ssn	Microsoft Windows netbios-ssn	cpe:/o:microsoft:windows
443	http	Apache httpd	cpe:/a:apache:http_server:2.4.41
445			
902			
912			
2869	http	Microsoft HTTPAPI httpd	cpe:/o:microsoft:windows
3306	mysql	MariaDB	cpe:/a:mariadb:mariadb

192.168.0.1 || 28:3B:82:64:37:B7			
CVEName	**AttackType**	**Score**	**AccessVector**
cve-2017-15107	unknown	5	network
cve-2011-4362	denialofservice	5	network
cve-2013-1427	unknown	1.9	local
cve-2013-4559	allowsremoteattackersto	7.6	network
cve-2013-4560	denialofservice	2.6	network
cve-2014-2323	remoteexecode	7.5	network
cve-2014-2324	remoteattacker	5	network
cve-2018-19052	unknown	5	network
cve-2010-0295	denialofservice	5	network

192.168.0.208 ||			
CVEName	**AttackType**	**Score**	**AccessVector**
cve-2009-3864	allowsremoteattackersto	7.5	network
cve-2011-3310	allowsremoteauthenticated	9	network
cve-2011-3389	unknown	4.3	network
cve-2011-0638	unknown	6.9	local
cve-2013-0894	bufferoverflow	7.5	network
cve-2014-2608	allowslocaluserstoobtain	2.1	local
cve-2014-8445	denialofservice	10	network
cve-2014-8446	denialofservice	10	network
cve-2014-8447	denialofservice	10	network
cve-2014-8448	unknown	5	network
cve-2014-8449	unknown	10	network
cve-2014-8451	unknown	5	network
cve-2014-8452	remoteattacker	5	network
cve-2014-8453	remoteattacker	5	network
cve-2014-8454	unknown	10	network
cve-2014-8455	unknown	10	network
cve-2014-8456	denialofservice	10	network
cve-2014-8457	bufferoverflow	10	network
cve-2014-8458	denialofservice	10	network
cve-2014-8459	denialofservice	10	network
cve-2014-8460	bufferoverflow	10	network

192.168.0.208 ||			
CVEName	**AttackType**	**Score**	**AccessVector**
cve-2014-8461	denialofservice	10	network
cve-2014-9158	denialofservice	10	network
cve-2014-9159	bufferoverflow	10	network
cve-2014-9160	bufferoverflow	10	network
cve-2014-9165	unknown	10	network
cve-2015-0312	unknown	10	network
cve-2015-1209	denialofservice	7.5	network
cve-2015-1210	allowsremoteattackersto	5	network
cve-2015-1211	allowsremoteattackersto	7.5	network
cve-2015-1212	denialofservice	7.5	network
cve-2015-3046	denialofservice	10	network
cve-2015-3047	denialofservice	5	network
cve-2015-3048	bufferoverflow	10	network
cve-2015-3049	denialofservice	10	network
cve-2015-3050	denialofservice	10	network
cve-2015-3051	denialofservice	10	network
cve-2015-3052	denialofservice	10	network
cve-2015-3053	unknown	10	network
cve-2015-3054	unknown	10	network
cve-2015-3055	unknown	7.5	network
cve-2015-3056	denialofservice	10	network
cve-2015-3057	denialofservice	10	network
cve-2015-3058	unknown	5	network
cve-2015-3059	unknown	10	network
cve-2015-3060	unknown	10	network
cve-2015-3061	unknown	10	network
cve-2015-3062	unknown	10	network
cve-2015-3063	unknown	10	network
cve-2015-3064	unknown	10	network
cve-2015-3065	unknown	10	network
cve-2015-3066	unknown	10	network
cve-2015-3067	unknown	10	network
cve-2015-3068	unknown	10	network

192.168.0.208 ||			
CVEName	**AttackType**	**Score**	**AccessVector**
cve-2015-3069	unknown	10	network
cve-2015-3070	denialofservice	10	network
cve-2015-3071	unknown	10	network
cve-2015-3072	unknown	10	network
cve-2015-3073	unknown	10	network
cve-2015-3074	unknown	10	network
cve-2015-3075	unknown	10	network
cve-2015-3076	denialofservice	10	network
cve-2015-4716	allowsremoteattackersto	10	network
cve-2015-4796	allowsremoteauthenticated	9	network
cve-2016-1715	denialofservice	5.5	local
cve-2016-4158	localrootexploit	6.9	local
cve-2016-4534	unknown	3	local
cve-2010-3139	remoteattacker	9.3	network
cve-2010-3143	remoteattacker	9.3	network
cve-2008-6194	denialofservice	7.8	network
cve-2010-3888	localrootexploit	7.2	local
cve-2010-3889	localrootexploit	7.2	local
cve-2007-2108	allowsremoteattackersto	6.8	network
cve-2016-6664	unknown	6.9	local

192.168.0.1 || 28:3B:82:64:37:B7			
ID	**File**	**Desc**	**Date**
18295	exploits/linux/dos/18295.txt	lighttpd - Denial of Service (PoC)	2011-12-31
33591	exploits/linux/dos/33591.sh	lighttpd 1.4/1.5 - Slow Request Handling Remote Denial of Service	2010-02-02

192.168.0.208 ||			
ID	**File**	**Desc**	**Date**
38344	exploits/windows/dos/38344.txt	Adobe Acrobat Reader - AFParseDate JavaScript API Restrictions Bypass	2015-09-28
14733	exploits/windows/local/14733.c	Microsoft Windows 7 - 'wab32res.dll wab.exe' DLL Hijacking	2010-08-24
14745	exploits/windows/local/14745.c	Microsoft Address Book 6.00.2900.5512 - 'wab32res.dll' DLL Hijacking	2010-08-25

192.168.0.208 ||			
ID	**File**	**Desc**	**Date**
14758	exploits/windows/local/14758.c	Microsoft Group Convertor - 'imm.dll' DLL Hijacking	2010-08-25
14778	exploits/windows/local/14778.c	Microsoft Windows - Contacts 'wab32res.dll' DLL Hijacking	2010-08-25
15589	exploits/windows/local/15589.wsf	Microsoft Windows - Task Scheduler Privilege Escalation	2010-11-20
19930	exploits/windows/local/19930.rb	Microsoft Windows - Task Scheduler '.XML' Local Privilege Escalation (MS10-092) (Metasploit)	2012-07-19
39531	exploits/windows/local/39531.c	McAfee VirusScan Enterprise 8.8 - Security Restrictions Bypass	2016-03-07
40679	exploits/linux/local/40679.sh	MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7.x - 'root' System User Privilege Escalation	2016-11-01