CHECK POINT
MISFORTUNE COOKIE – SUSPECTED VULNERABLE MODEL LIST

WHAT IS THE MISFORTUNE COOKIE VULNERABILITY?

Misfortune Cookie is a critical vulnerability that allows an intruder to remotely take over a residential gateway device and use it to attack the devices connected to it.

Researchers from Check Point's Malware and Vulnerability Research Group recently uncovered this critical vulnerability present on millions of residential gateway (SOHO router) devices from different models and makers. It has been assigned the CVE-2014-9222 identifier. This severe vulnerability allows an attacker to remotely take over the device with administrative privileges.

HOW MANY DEVICES ARE AFFECTED?

To date, researchers have distinctly detected at least 12 million readily exploitable devices connected to the Internet present in 189 countries across the globe, making this one of the most widespread vulnerabilities revealed in recent years.

HOW DOES IT AFFECT ME?

If your gateway device is vulnerable, then any device connected to it - including computers, phones, tablets, printers, security cameras, refrigerators, toasters or any other networked device in your home or office network - may have increased risk of compromise. An attacker exploiting the Misfortune Cookie vulnerability can easily monitor your Internet connection, steal your credentials and personal or business data, attempt to infect your machines with malware, and over-crisp your toast.

IS IT THAT BAD?

Yes.

WHICH MODELS ARE AFFECTED? AM I AFFECTED?

Prior to this publication and the expected firmware patches, we believe that devices containing RomPager services with versions before 4.34 (and specifically 4.07) are vulnerable. Note that some vendor firmware updates may patch RomPager to fix Misfortune Cookie without changing the displayed version number, invalidating this as an indicator of vulnerability.

HOW WAS THIS LIST COMPILED?

The task of fingerprinting online devices is a challenging one. Devices may or may not contain an identifying banner as a response for an unauthenticated user. The banner may include a model number, a brand name, or a simple welcome message that makes it hard to identify the underlying hardware.

To make things even more challenging, manufacturers and ISPs commonly rebrand a device using different names and model numbers per distribution location or product series.

The following list was collected through Internet-wide scanning on various ports. When we detected a response from a suspected vulnerable RomPager service, we added the HTTP authentication realm to our list, which typically contained a model number for the device.

Brand names were collected using online search results for the model numbers.

This does not mean all firmware versions of the device are vulnerable. It means at least one version of that device seemed vulnerable during our scans, performed November 2014.

The list is therefore by no means complete, exhaustive, or error-proof. We did not attempt to test or verify on all models, as we do not own every model in our lab. Please contact your device manufacturer (or ISP in case of ISP-provided equipment) to check if your model is vulnerable to Misfortune Cookie.

This list was last updated at December 22, 2014, 12:11 GMT

SUSPECTED-VULNERABLE MODELS

110TC2	Beetel	BW554	SBS
16NX073012001	Nilox	C300APRA2+	Conceptronic
16NX080112001	Nilox	Compact Router ADSL2+	Compact
16NX080112002	Nilox	D-5546	den-it
16NX081412001	Nilox	D-7704G	den-it
16NX081812001	Nilox	Delsa Telecommunication	Delsa
410TC1	Beetel	D-Link_DSL-2730R	D-Link
450TC1	Beetel	DM 856W	Binatone
450TC2	Beetel	DSL-2110W	D-Link
480TC1	Beetel	DSL-2120	D-Link
AAM6000EV/Z2	ASUS	DSL-2140	D-Link
AAM6010EV	ASUS	DSL-2140W	D-Link
AAM6010EV/Z2	ASUS	DSL-2520U	D-Link
AAM6010EV-Z2	ASUS	DSL-2520U_Z2	D-Link
AAM6020BI	ASUS	DSL-2600U	D-Link
AAM6020BI-Z2	ASUS	DSL-2640R	D-Link
AAM6020VI/Z2	ASUS	DSL-2641R	D-Link
AD3000W	starnet	DSL-2680	D-Link
ADSL Modem	Unknown	DSL-2740R	D-Link
ADSL Modem/Router	Unknown	DSL-320B	D-Link
ADSL Router	BSNL	DSL-321B	D-Link
AirLive ARM201	AirLive	DSL-3680	D-Link
AirLive ARM-204	AirLive	DT 815	Binatone
AirLive ARM-204 Annex A	AirLive	DT 820	Binatone
AirLive ARM-204 Annex B	AirLive	DT 845W	Binatone
AirLive WT-2000ARM	AirLive	DT 850W	Binatone
AirLive WT-2000ARM Annex A	AirLive	DWR-TC14 ADSL Modem	Unknown
AirLive WT-2000ARM Annex B	AirLive	EchoLife HG520s	Huawei
AMG1001-T10A	ZyXEL	EchoLife Home Gateway	Huawei
APPADSL2+	Approx	EchoLife Portal de Inicio	Huawei
APPADSL2V1	Approx	GO-DSL-N151	D-Link
AR-7182WnA	Edimax	HB-150N	Hexabyte
AR-7182WnB	Edimax	HB-ADSL-150N	Hexabyte
AR-7186WnA/B	Edimax	Hexabyte ADSL	Hexabyte
AR-7286WNA	Edimax	Home Gateway	Huawei
AR-7286WnB	Edimax	iB-LR6111A	iBall
Arcor-DSL WLAN-Modem 100	Arcor	iB-WR6111A	iBall
Arcor-DSL WLAN-Modem 200	Arcor	iB-WR7011A	iBall
AZ-D140W	Azmoon	iB-WRA150N	iBall
Billion Sky	Billion	iB-WRA300N	iBall
BiPAC 5102C	Billion	iB-WRA300N3G	iBall
BiPAC 5102S	Billion	IES1248-51	ZyXEL
BiPAC 5200S	Billion	KN.3N	Kraun
BIPAC-5100 ADSL Router	Billion	KN.4N	Kraun
BLR-TX4L	Buffalo	KR.KQ	Kraun

KR.KS	Kraun	POSTEF-8840	Postef
KR.XL	Kraun	POSTEF-8880	Postef
KR.XM	Kraun	Prestige 623ME-T1	ZyXEL
KR.XM\t	Kraun	Prestige 623ME-T3	ZyXEL
KR.YL	Kraun	Prestige 623R-A1	ZyXEL
Linksys BEFDSR41W	Linksys	Prestige 623R-T1	ZyXEL
LW-WAR2	LightWave	Prestige 623R-T3	ZyXEL
M-101A	ZTE	Prestige 645	ZyXEL
M-101B	ZTE	Prestige 645R-A1	ZyXEL
M-200 A	ZTE	Prestige 650	ZyXEL
M-200 B	ZTE	Prestige 650H/HW-31	ZyXEL
MN-WR542T	Mercury	Prestige 650H/HW-33	ZyXEL
MS8-8817	SendTel	Prestige 650H-17	ZyXEL
MT800u-T ADSL Router	BSNL	Prestige 650H-E1	ZyXEL
MT880r-T ADSL Router	BSNL	Prestige 650H-E3	ZyXEL
MT882r-T ADSL Router	BSNL	Prestige 650H-E7	ZyXEL
MT886	SmartAX	Prestige 650HW-11	ZyXEL
mtnlbroadband	MTNL	Prestige 650HW-13	ZyXEL
NetBox NX2-R150	Nilox	Prestige 650HW-31	ZyXEL
Netcomm NB14	Netcomm	Prestige 650HW-33	ZyXEL
Netcomm NB14Wn	Netcomm	Prestige 650HW-37	ZyXEL
NP-BBRsx	Iodata	Prestige 650R-11	ZyXEL
OMNI ADSL LAN EE(Annex A)	ZyXEL	Prestige 650R-13	ZyXEL
P202H DSS1	ZyXEL	Prestige 650R-31	ZyXEL
P653HWI-11	ZyXEL	Prestige 650R-33	ZyXEL
P653HWI-13	ZyXEL	Prestige 650R-E1	ZyXEL
P-660H-D1	ZyXEL	Prestige 650R-E3	ZyXEL
P-660H-T1 v3s	ZyXEL	Prestige 650R-T3	ZyXEL
P-660H-T3 v3s	ZyXEL	Prestige 652H/HW-31	ZyXEL
P-660HW-D1	ZyXEL	Prestige 652H/HW-33	ZyXEL
P-660R-D1	ZyXEL	Prestige 652H/HW-37	ZyXEL
P-660R-T1	ZyXEL	Prestige 652R-11	ZyXEL
P-660R-T1 v3	ZyXEL	Prestige 652R-13	ZyXEL
P-660R-T1 v3s	ZyXEL	Prestige 660H-61	ZyXEL
P-660R-T3 v3	ZyXEL	Prestige 660HW-61	ZyXEL
P-660R-T3 v3s	ZyXEL	Prestige 660HW-67	ZyXEL
P-660RU-T1	ZyXEL	Prestige 660R-61	ZyXEL
P-660RU-T1 v3	ZyXEL	Prestige 660R-61C	ZyXEL
P-660RU-T1 v3s	ZyXEL	Prestige 660R-63	ZyXEL
P-660RU-T3 v3s	ZyXEL	Prestige 660R-63/67	ZyXEL
PA-R11T	Solwise	Prestige 791R	ZyXEL
PA-W40T-54G	PreWare	Prestige 792H	ZyXEL
Cerberus P 6311-072	Pentagram	RAWRB1001	Reconnect
PL-DSL1	PreWare	RE033	Roteador
PN-54WADSL2	ProNet	RTA7020 Router	Maxnet
PN-ADSL101E	ProNet	RWS54	Connectionnc
Portal de Inicio	Huawei	SG-1250	Everest

SG-1500	Everest	TD-W8901G 3.0	TP-Link
SmartAX	SmartAX	TD-W8901GB	TP-Link
SmartAX MT880	SmartAX	TD-W8901N	TP-Link
SmartAX MT882	SmartAX	TD-W8951NB	TP-Link
SmartAX MT882r-T	SmartAX	TD-W8951ND	TP-Link
SmartAX MT882u	SmartAX	TD-W8961N	TP-Link
Sterlite Router	Sterlite	TD-W8961NB	TP-Link
Sweex MO300	Sweex	TD-W8961ND	TP-Link
T514	Twister	T-KD318-W	MTNL
TD811	TP-Link	TrendChip ADSL Router	BSNL
TD821	TP-Link	UM-A+	Asotel
TD841	TP-Link	Vodafone ADSL Router	BSNL
TD854W	TP-Link	vx811r	CentreCOM
TD-8616	TP-Link	WA3002-g1	BSNL
TD-8811	TP-Link	WA3002G4	BSNL
TD-8816	TP-Link	WA3002-g4	BSNL
TD-8816 1.0	TP-Link	WBR-3601	LevelOne
TD-8816 2.0	TP-Link	WebShare 111 WN	Atlantis
TD-8816B	TP-Link	WebShare 141 WN	Atlantis
TD-8817	TP-Link	WebShare 141 WN+	Atlantis
TD-8817 1.0	TP-Link	Wireless ADSL Modem/Router	Unknown
TD-8817 2.0	TP-Link	Wireless-N 150Mbps ADSL Router	BSNL
TD-8817B	TP-Link		
TD-8820	TP-Link	ZXDSL 831CII	ZTE
TD-8820 1.0	TP-Link	ZXDSL 831II	ZTE
TD-8840T	TP-Link	ZXHN H108L	ZTE
TD-8840T 2.0	TP-Link	ZXV10 W300	ZTE
TD-8840TB	TP-Link	ZXV10 W300B	ZTE
TD-W8101G	TP-Link	ZXV10 W300D	ZTE
TD-W8151N	TP-Link	ZXV10 W300E	ZTE
TD-W8901G	TP-Link	ZXV10 W300S	ZTE