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.

SUSPECTED-VULNERABLE MODELS

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

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

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