Adobe Patches 43 Flaws Across Eight Products

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/a5-ChrTsR_M/adobe-patches-43-flaws-across-eight-products

---

Verizon Patches Vulnerabilities Affecting Millions of Routers

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/6U8L7WHdFOg/verizon-patches-vulnerabilities-affecting-millions-routers

---

Unofficial Patch Released for Java Flaws Found by Google Researcher

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/sl8kicbbx6M/unofficial-patch-released-java-flaws-found-google-researcher

Rockwell Patches Stratix Switch Flaws Introduced by Cisco Software

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/dBOmYX4gztM/rockwell-patches-stratix-switch-flaws-introduced-cisco-software

Ongoing DNS hijackings target unpatched consumer routers

reader comments

5 with 5 posters participating

Share this story

A wave of DNS hijacking attacks that abuse Google’s cloud computing service is causing consumer routers to connect to fraudulent and potentially malicious websites and addresses, a security researcher has warned.

By now, most people know that Domain Name System servers

translate human-friendly domain names into the numeric IP addresses that computers need to find other computers on the Internet. Over the past four months, a blog post published Thursday said, attackers have been using Google cloud service to scan the Internet for routers that are vulnerable to remote exploits. When they find susceptible routers, the attackers then use the Google platform to send malicious code that configures the routers to use malicious DNS servers.

Troy Mursch, the independent security researcher who published Thursday's post, said the first wave hit in late December. The campaign exploited vulnerabilities in four models of D-Link routers, including:

The exploits gave attackers control over routers that hadn't been patched. The attackers would then use their control to reconfigure the routers to use a DNS server at 66.70.173.48, an IP address provided by host OVH.

A second wave in early February targeted the same vulnerable D-Link routers, only this time it caused them to use a rogue DNS server at 144.217.191.145, a different OVH IP address. According to Twitter user parseword, most of the DNS requests were then redirected to two IPs, one allocated to a crime-friendly hosting provider (AS206349) and the other pointing to a service that monetizes parked domain names (AS395082).

The third and last-known wave occurred last week. It came from three distinct Google Cloud Platform hosts and targeted additional consumer router models including the ARG-W4 ADSL, DSLink 260E, and those from Secutech and TOTOLINK. The rogue DNS servers used in the latest round, 195.128.126.165 and 195.128.124.131, are both hosted in Russia by Inoventica Services, with Internet access being provided by subsidiary Garant-Park-Internet Limited (AS47196).

At the time this post was being written, the last batch of rogue DNS servers was still operating, Mursch told Ars. The

DNS servers from the previous waves, he added, were no longer operating. While the attacks abused services from a variety of providers, Mursch said Google's cloud service stood out.

"It's not meant to be a Google hit piece," the researcher said of Thursday's post. "But it's so trivial to abuse their platform. You sign up for an account and boom. It really is that easy." He said Google will eventually terminate service once the company receives reports of the abuse, but it often takes time and effort before that happens. Ars asked Google representatives for comment and will update this post if they respond.

Mursch said he hasn't yet investigated precisely what domains are spoofed in the attacks. One of the best-known DNS hijacking campaigns came to light in 2012 under the name DNS Changer and generated millions of dollars in fake advertising revenue by steering 500,000 computers to fake addresses. Rogue DNS server schemes have also been used to surreptitiously serve malicious ads and direct people to fake banking sites.

The best way for people to protect themselves against these sorts of attacks is to ensure their routers are running the latest firmware. All four of the D-Link vulnerabilities under attack were fixed years ago, but many people never go through the hassle of manually installing the patches. It's also a good idea to periodically inspect router configurations to make sure DNS settings are OK. Cloudflare's free DNS service 1.1.1.1 is a good bet. It's never a bad idea to also configure the operating system of each device to use a DNS server such as 1.1.1.1, but Mursch warned that sometimes malicious changes made to hacked routers can override those OS configurations.

https://arstechnica.com/?p=1486635

NVIDIA Patches High Severity Flaws in Tegra Drivers

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/_PmtBaJPxi4/nvidia-patches-high-severity-flaws-tegra-drivers

---

Cisco Patches Router Vulnerabilities Targeted in Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/mH8gNtDmEjQ/cisco-patches-router-vulnerabilities-targeted-attacks

---

Microsoft Not Concerned About Disclosed Edge, IE Flaws

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/kyQhidDfF74/microsoft-not-concerned-about-disclosed-edge-ie-flaws

Microsoft Paid $2,000,000 in Bounty Rewards in 2018

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/K9o0HrWFT78/microsoft-paid-2000000-bounty-rewards-2018

Google Patches Critical Vulnerabilities in Android’s Media Framework

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/9OM6lD9vVNI/google-patches-critical-vulnerabilities-androids-media-framework