SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- Suits and Spooks

Security Experts:

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe (Free)
- Security White Papers
- ICS Cyber Security Conference
- Contact Us

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - White Papers
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
  - Whitepapers
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
  - Whitepapers
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - White Papers
  - Network Security
  - Application Security
- Management & Strategy

Unpatched Flaws Allow Hackers to Compromise Belkin Routers

By Eduard Kovacs on December 01, 2015

A researcher has published the details and proof-of-concept (PoC) code for several unpatched vulnerabilities affecting Belkin's N150 wireless home routers.

The security bugs were discovered in October by Rahul Pratap Singh, an India-based researcher whose work has been acknowledged by several major companies, including Microsoft, Adobe, eBay, ESET and Google.

One of the vulnerabilities found by Singh is an HTML/script injection that affects the "language" parameter present in the request sent to the router. A video demo published by the expert shows that injecting a payload into the parameter causes the device's web interface to become unusable.

The researcher also discovered a session hijacking issue caused by the fact that the session ID is a hexadecimal string with a fixed length of eight characters. This allows an attacker to easily obtain the data via a brute force attack.

One major security weakness in Belkin N150 wireless routers is related to the Telnet protocol, which is enabled with the default username/password combination root/root. The vulnerability allows a malicious hacker to gain remote access to the router with root privileges, Singh said.

The researcher also determined that requests sent to the router can be manipulated due to the lack of cross-site request forgery (CSRF) protection.

Singh noted that while some of these vulnerabilities require a direct connection, others, like the CSRF flaw, can be exploited remotely.

"A combination of these vulnerabilities will lead to a full compromise of the router," Singh told *SecurityWeek* via email.

"An attacker may have a machine on the local network, either by physically connecting, or by compromising a machine on the local network through other means (e.g. via malware). Then it can use telnet to do the rest of the stuff to compromise the router," Singh explained. "Same can be done using the CSRF vulnerability to perform malicious actions."

The researcher says the vulnerabilities affect firmware version 1.00.09 (F9K1009) which, according to Belkin's official support page for N150 routers, is the latest version available for this device model. The issues were reported to the vendor on October 20 and again on November 25. Since he hasn't received any response from the company, Singh says he has been advised by US-CERT to make his findings public.

Singh told *SecurityWeek* that he has requested CVE identifiers for the vulnerabilities.

Judging by the changelog on the Belkin N150 support page, the company rarely releases security updates for the device. Version 1.00.08 was released in May 2014 to address one security issue and version 1.00.09 was released in May 2015 to patch a "NAT-PMP security vulnerability."

The issue Belkin attempted to resolve with the release of version 1.00.08 is likely a high severity path traversal vulnerability (CVE-2014-2962) reported in March 2014 by Aditya Lad. Singh later discovered that the vendor failed to properly patch the flaw, which has been found to affect version 1.00.09 of the firmware as well.

Belkin told *SecurityWeek* that the company is aware of the security issues affecting F9K1009 v1 N150 routers and is working to address them.

**Updated to say that Belkin is working on patching the vulnerabilities*

Related Reading: Details Disclosed for Buffer Overflow Vulnerability in Belkin Routers

Previous Columns by Eduard Kovacs:
Over 6 Million Kids Profiles Accessed in VTech Hack
Malware Used by China APT Group Abuses Dropbox
Unpatched Flaws Allow Hackers to Compromise Belkin Routers
Schneider Patches RCE Flaws in ProClima Software
Videofied Alarm System Flaws Allow Hackers to Intercept Data

Tags:
Network Security NEWS & INDUSTRY

ALSO ON SECURITYWEEK PROVIDES INFORMATION SECURITY NEWS AND ANALYSIS. WHAT'S THIS?

Flaws in Rockwell PLCs Expose Operational Networks

1 comment • a month ago

Jossef Harush — YAY! i love you guys!

Researcher Demonstrates Simple BitLocker Bypass

1 comment • 14 days ago

Hexstr Morgan — "For the exploit to be successful, however, BitLocker on the target system has to be enabled without a PIN or …

ProtonMail Suspects State-Sponsored DDoS Attack

3 comments • a month ago

Timothy — Is it possible for them to find out which country this is originating from?

Android Adware Abuses Accessibility Service to Install Apps

1 comment • 12 days ago

Graham — PureVPN's Android VPN helps you smash every restriction, blockage, censorship & online threat to pieces. Get it …

Most Recent Most Read

- Over 6 Million Kids Profiles Accessed in VTech Hack
- China Blamed as Australia's Weather Bureau Hacked: Report
- Malware Used by China APT Group Abuses Dropbox
- Unpatched Flaws Allow Hackers to Compromise Belkin Routers
- Schneider Patches RCE Flaws in ProClima Software
- ThreatConnect Closes $16 Million Series B Funding
- BlackBerry Exits Pakistan Over Backdoor Request
- Chased by the Dragon: Containment is the New Detection
- Videofied Alarm System Flaws Allow Hackers to Intercept Data
- US Ends Bulk Collection of Phone Data

Popular Topics

Information Security News
IT Security News
Risk Management
Cybercrime
Cloud Security
Application Security
Smart Device Security

Security Community

IT Security Newsletters
IT Security White Papers
Suits and Spooks
ICS Cyber Security Conference
CISO Forum
InfosecIsland.Com

Stay Intouch

Twitter
Facebook
LinkedIn Group
Cyber Weapon Discussion Group
RSS Feed
Submit Tip
Security Intelligence Group

About SecurityWeek

Team
Advertising
Events
Writing Opportunities
Feedback
Contact Us