

Trusted Foundation.

The storage foundation

Learn more >



The New InfoWorld App Dev Cloud Mobile Open Source Security Deep Dives Reviews Resources

Rows

InfoWorld

Search

chat  
share

# Backdoor found in D-Link router firmware code

The backdoor could be used to modify a router's settings -- a dangerous vulnerability

By Jeremy Kirk

IDG News Service | Oct 14, 2013

A backdoor found in firmware used in several D-Link routers could allow an attacker to change a device's settings, a serious security problem that could be used for surveillance.

**Craig Heffner**, a vulnerability researcher with Tactical Network Solutions who specializes in wireless and embedded systems, found the vulnerability. Heffner wrote on his **blog** that the Web interface for some D-Link routers could be accessed if a browser's user agent string is set to `xmlset_roodkcableoj28840ybtide`.

**[ Prevent corporate data leaks with Roger Grimes' "Data Loss Prevention Deep Dive" PDF expert guide, only from InfoWorld. | Stay up to date on the latest security developments with InfoWorld's Security Central newsletter. ]**

Curiously, if the second half of the user agent string is reversed and the number is removed, it reads "edit by joel backdoor," suggesting it was intentionally placed there.

"My guess is that the developers realized that some programs/services needed to be able to change the device's settings automatically," Heffner wrote. "Realizing that the Web server already had all the code to change these settings, they decided to just send requests to the Web server whenever they needed to change something.

"The only problem was that the Web server required a username and password, which the end user could change. Then, in a eureka moment, Joel jumped up and said, 'Don't worry, for I have a cunning plan!'"

The technology industry has been rattled by documents leaked by former NSA contractor Edward Snowden, which indicate the spy agency pursues ways to subvert security measures through backdoors. But developers sometimes make mistakes and in other cases, make poor security decisions.

With access to a router's settings, an attacker could potentially steer someone's Internet traffic through another their own server and read their unencrypted data traffic.

To find other vulnerable D-Link router models, Heffner used a special search engine called [Shodan](#), which is designed to find any device connected to the Internet, ranging from refrigerators to CCTV cameras to routers.

The affected models likely include D-Link's DIR-100, DI-524, DI-524UP, DI-604S, DI-604UP, DI-604+, TM-G5240 and possibly the DIR-615. The same firmware is also used in the BRL-04UR and BRL-04CW routers made by Planex, Heffner wrote.

A Web search turned up the suspicious user agent string in a post on a Russian forum three years ago, Heffner wrote, which means somebody has known about it for a while.

D-Link officials could not be immediately reached for comment on Monday.

*Send news tips and comments to [jeremy\\_kirk@idg.com](mailto:jeremy_kirk@idg.com). Follow me on Twitter: [@jeremy\\_kirk](#).*

**Follow everything from InfoWorld**

[Twitter](#)[Facebook](#)[LinkedIn](#)[Google+](#)[RSS](#)

RECOMMENDED

- Court throws out \$368.2 million patent award against Apple
- A lower court made mistakes in defining the value of the patented technology asserted by VirnetX,...
- Video: Find out what's new in C# 6.0
- C# vNext, better known as version 6.0 of the venerable programming language, is on the way. Here's...
  - 10 ways to query Hadoop with SQL



Dropbox taps C++ for mobile app dev

**BRANDPOST**

Sponsored by Rackspace

How is Downtime Impacting Your Bottom Line?

**VIDEO/WEBCAST**

Sponsored

Big Data in the Mainstream: Insights for Everyone, Everywhere

In this Webcast you will learn why small data is important and how to embed insights into CRM and...

**JOIN THE DISCUSSION**

---

**MOST READ**

---

**7 reasons Apple should open-source Swift -- and 7 reasons it won't**

Faster innovation, better security, new markets -- the case for opening Swift might be more compelling



**The 5 lessons both IT and business should learn from Apple**



**5 reasons why hackers own your organization**

**NEWSLETTERS**

---

Sign up and receive the latest news, reviews and trends on your favorite technology topics.

Get our Daily News Newsletter:

Go

Facebook's TODO project is a big push to evolve the world of open source

The project aims to improve how open source software is developed and consumed

Welcome to the new InfoWorld

Does something seem a little different? It's an entirely new design, but the same great enterprise tech

BRANDPOST

[Learn more](#)

SPONSORED BY Rackspace

Cloud Tools to Enhance Your Application Performance

RESOURCES

VIDEO/WEBCAST

SPONSORED



Big Data in the Mainstream: Insights for Everyone, Everywhere



**WHITE PAPER**

**BYOD doesn't have to be a pain in your B-U-T-T**

WHITE PAPER

Harness the power of personal smartphones with BYOD



WHITE PAPER

Leverage the Power of APIs to Turbocharge Your Mobile Strategy: 7 Steps to a Successful API Program

WHITE PAPER

Tame BYOD. Simplify MDM. Empower today's Can-Do IT.

Go

TOP STORIES

5 reasons why hackers own your organization

The Target and Home Depot breaches should've been wake-up calls. Instead, the bad guys remain free to



What to expect from Windows

With Build 9834 leaks and confirmations springing up all over, here's what to expect from Microsoft on

Welcome to the new InfoWorld

Does something seem a little different? It's an entirely new design, but the same great enterprise tech

The 5 lessons both IT and business should learn from Apple

Tired of being ineffective and unloved? It's time to act different



If you're an Apple admin, you won't want to miss the 2014 JNUC.

JAMF Software makes BYOD finally manageable with the Casper Suite



Virtualize your Tier-1 Applications Today! Watch the Webcast!

# InfoWorld

[Twitter](#) [LinkedIn](#) [Facebook](#) [Google+](#) [RSS](#) 

[Application Development](#) [Applications](#) [Big Data](#) [Cloud Computing](#) [Data Center](#) [Databases](#) [IT Careers](#) [Internet](#) [Linux](#)  
[Microsoft Windows](#) [Mobile Technology](#) [Networking](#) [Open Source Software](#) [Security](#)

[News](#) [Blogs](#) [Reviews](#) [Insider](#) [Resources](#) [Newsletters](#)

[ABOUT](#) [USCONTACT](#) [PRIVACY](#) [POLICY](#) [ADVERTISING](#) [CAREERS](#) [AT IDG](#) [SITE](#) [MAP](#) [AD](#) [CHOICES](#)

Copyright © 1994 - 2014 InfoWorld, Inc. All rights reserved.

Explore the IDG Network

descend