PRESENTED BY

TRACK 0 DETAILS

The objective in this contest is to demonstrate previously unidentified vulnerabilities in off-the-shelf consumer wireless routers. Contestants must provide relevant exploit information to the judges and publicly demonstrate the attack in the contest area.

Legal & Ethics

Only hack products that you own, or with the explicit permission of the owner.

Never have third parties connect to a device while you are testing it. All parties involved should be given informed consent.

It is your responsibility to ensure that your testing does not violate any licensing agreements (EULAs).

You must responsibily disclose any vulnerabilities that you discover.

Rules

Step 1. Identify and exploit a vulnerability

The vulnerability must be found in one of the listed routers (below) of the specified make, model, and firm-ware versions. You have from now until you register to identify and exploit vulnerabilities in one of these routers.

The vulnerability must be a 0-day vulnerability. That is, it must not be previously disclosed to the public.

Vulnerability chaining is great! The more powerful your attack, the higher you will score. Combine your 0-day with other 0-days or known issues.

Step 2. Register to compete

Contestants will be judged on a first come, first serve basis – so register early. If someone else has an earlier time slot than you and demonstrates the same vulnerability before your turn, you may not be subject to a prize. When you select your time slot, you must provide some details about your exploit, but may withhold full details until the contest presentation.

Step 3. Demonstrate your exploit

If you've registered for the contest, you will have been assigned a time slot. Please show up during your assigned time slot, or your entry may be forfeited.

Your demonstration slot will have a limited time window, and if you fail to demonstrate the exploit successfully within that window, you may be disqualified.

At the time of demonstration, you must provide full exploit details.

At the time of the demonstration, routers will be factory reset with the specified firmware loaded and administrative password changed.

Registering

To register for track 0, please fill out the registration form located **here**.

Routers

The following routers and firmware versions may be used.

Linksys EA6500 [Ver.1.1.40 (build 160989)]

ASUS RT-AC66U (HW Ver. A2) [Version 3.0.0.4.374.5517]

TRENDnet TEW-812DRU (H/W: v1.0R) [Version 2.0.6.0]

Netgear Centria WNDR4700 [Version V1.0.0.52]

Netgear WNR3500U/WNR3500L [Version V1.2.2.48_35.0.55]

TP-Link TL-WR1043ND (Ver. 1.10) [Version V1_140319]

D-Link DIR-865L (HW Ver. A1) [Version 1.05]

Belkin N900 DB (Model: F9K1104v1) [Version 1.00.23]
EFF Open Wireless Router [Details forthcoming]

Awards

Prizes will be announced soon.

Guru compromise. Must score 5000 points – essentially, demostrate the most powerful attack in all categories with no caveats. We've put in for black badge, but no gaurantees.

1337 compromise. Must score 3000 points – pretty damn close to grand prize, but constrained by falling short from most powerful in any category, or having sufficient caveats to make the real world application of this attack less likely.

Rabble rouser compromise. Must score 1000 points – less damaging attacks than full control, but still represent significant security compromises.

Still good compromise. Must score 100 points – weaker attacks, but exploits nevertheless.

You may submit multiple exploits, compete multiple times, and win multiple and duplicative awards.

Scoring

All vulnerabilities are welcome, but winners will be determined based on various criteria.

Damage (Scoring). Attacks that demonstrate significant damage are scored higher than weaker attacks.

Full router control: 5000 points
Unprivileged/partial control: 4000 points
Corruption/compromise internal network: 4000 points
Modification of router behavior or controls: 3000 points
High-value* information leakage: 3000 points
Bricking: 3000 points
Denial of Service: 1000 points
Low-value** information leakage: 1000 points.
High-value information may include administrative or other passwords, user files, network

information, etc.

Low-value information may include router-specific information, such as router name, user names, etc., but nothing that would ordinarily have value on its own.

Penalties. Attacks that require special conditions and caveats are subject to point reductions.

Non-remote attack: -1000 points

Requires human interaction: -1000 points

Requires authenticated session: -1000 points

Requires administrative password: -1000 points

Requires other system/network information: -500 points

Requires special system configuration: -500 points

Relies on other special circumstances: -500 points

Exploit is unreliable: -500 points

Lack of post-exploit control: -500 points

Responsible Disclosure

This contest has a strict responsible disclosure policy, and responsible disclosure on the part of contestants is encouraged and supported. All 0-day vulnerabilities submitted to this contest must at some point be disclosed to the affected manufacturer prior to its demonstration at the contest area.

If I disclose the vulnerability to the manufacturer, will it still qualify as a 0-day?
Yes, but you must do so through the proper channels. You may submit your vulnerability details through Mitre, ZDI, etc., and even submit details of your vulnerability to the manufacturer. Just be sure to REGISTER YOUR EXPLOIT with our contest at the same time. This way, even if the manufacturer discloses the vulnerability prior to the contest you can still get full credit.

How can I trust you with these vulnerability details?
That's up to you. We're trustworthy guys, but you may not know us. You may withold essential vulnerability details at registration, but must disclose the full vulnerability at the contest. Just be sure to submit enough information that we can verify the authenticity of your claim at that time. We recommend you submit a cryptographic SHA-256 sum of your vulnerability write up at registration, so that we can verify you in fact had the full vulnerability details at that time.

Will you disclose vulnerability details prior to the contest? No. But if you've discovered something terrible, we will encourage you to do the right thing and tell the manufacturer as soon as possible.

Will you help me disclose a vulnerability prior to the contest? We can point you in the right direction, but for legal reasons you're essentially on your own.

What if I disclose the vulnerability details myself, will it still qualify as a 0-day at the contest? No.