Byos Bug Bounty Program: Hardwear.io Conference 2019

White Paper

Document version: 1.0
October 4th, 2019

1.0 - Introduction

1.1 - Summary

Over the course of four days, Security Researchers participated in our Bug Bounty at the HardPWN Hardware Hacking Competition during the Hardwear.io conference. There were no vulnerabilities found in the Byos Portable Secure Gateway Device. We attribute this to the improvements made to our internal SDLC processes after the first Vegas Bug Bounty.

1.2 - Objective

The overall objective of the bug bounty program is to validate the security claims of the Byos Portable Secure Gateway and to discover any existing vulnerabilities in the product and its features. Additional benefits include:

- Practising the company's internal vulnerability handling process
- Increasing our security team's awareness of how attackers approach the security mechanisms of the product
- Learning and validating security development best practices by having active feedback from researchers
- Gathering external expert opinions on the product's feature-set, benefits and use-cases

1.3 - Time and Location

The Bug Bounty took place from September 23-27, 2019, in The Hague, Netherlands at the Hardwear.io Hardware Hacking Conference.

1.4 - Participants

Over 250 people attended the Hardwear.io conference and 30 people attended the HardPWN Hardware Hacking Competition. Including the Portable Secure Gateway (PSG), the following products were also available for pentesting:

- Noke HD Bluetooth Smart Padlock
- Nest Cam IQ
- Google Nest Hub
- Nest Hello
- Nest Secure
- Nest Protect
- Google Home
- Chromecast
- Google WiFi
- MiNiBREW Craft System

Researchers spent time with each technology, trying to find vulnerabilities in them, then moving on to the next products. The list of researchers who tested the Byos PSG included:

- Adam Laurie
- Grzegorz Wypych
- Catherine Norcom
- Arun Magesh

1.5 - Reporting method

The participating researchers were required to submit a Proof of Concept (PoC) on the Zerocopter platform. To be able to claim a valid finding, the PoC needed to be immediately replicated by one of the Byos staff according to the technique reported by the researcher.

1.6 - Scope

The Bug Bounty was performed on the Byos PSG Beta-prototype. Each researcher was handed an individual device. The vectors of attack included:

- Hardware tampering
- Web-based attacks
- Network protection mechanism bypass

1.7 - Categories

The potential vulnerabilities were classified into different severity levels:

- **Low** - these vulnerabilities have no real impact on the security of the user, but do indicate a minor malfunction in functionality of the product.
  Some examples include: *XSS, CSRF, RFI, broken Web feature*

- **Medium** - these vulnerabilities can cause minimal damage to the user when executed.
  Some examples include: *Stored XSS, LFI, DDoS*

- **High** - these vulnerabilities expose the user's data and indicate flaws in product functionality and security.
  Some examples include: *IDOR, SSRF, Auth Bypass, Breaking the Encryption layer*

- **Critical** - a critical vulnerability is core to the functioning and protection offered by the Byos PSG, leaving the user at maximum exposure.
  Some examples include: *RCE, IDOR, SQLi, or a core protection mechanism bypass*

2.0 - Findings

Researchers were not able to find any vulnerabilities in the Portable Secure Gateway during this Bug Bounty event

3.0 - Conclusion

During our first Bug Bounty event in Vegas, there were a total of 8 vulnerabilities found; the Web Dashboard was subsequently hardened by adding new server-side validations to address input validations and database queries in the backend code, for all sections that involve user input.

Since our last Bug Bounty event, our team has implemented full SDLC practices into our internal development processes, including automated tests to identify future instances automatically, and parameterized SQL queries throughout our code.

Some of the additional specific improvements to the product included:

- Validation of inputs in the API
- The logic of the Wi-Fi connection from the API
- Flow of information between our proprietary 4-way API and the Front-End
- Hardening of the Web Server hosted in the Byos Portable Secure Gateway
- Status control of the Byos services running in the Byos Portable Secure Gateway

Researchers at the HardPWN bounty were also testing the improved existing features as well as new features implemented between August 15th -September 20th, 2019; these included:

- Multi-antenna WiFi Identification
- New function to enumerate and recognize all new ARP traffic on the network
- Block DNS queries initiated by the client device to foreign servers
- Detection and handling of captive portals
- Creation of a 3-layer signature process to validate known networks
- New dynamic Firewall rules
- WiFi Secure Auto Connect processes
- Network degradation checks

We believe it is a strong signal that none of the participants were able to find weaknesses in the product during this event. We attribute the lack of findings from this Bug Bounty as a result of the improvements made to our internal SDLC processes, which allowed us to identify and mitigate weak points within the product earlier on in the development process.

The next Byos Bug Bounty event will be conducted on the final product, with our fully proprietary hardware design. With the help of the global security community, we will continue to test and improve the Portable Secure Gateway through our ongoing bug bounty program.

4.0 - Footnotes

4.1 -Copyright & Trademarks

4.2 - Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Byos shall have no liability for any errors or damages of any kind resulting from the use of this document.

4.3 - Contact Information

Mkit North America Inc.
1505 Barrington St., Unit 100
Halifax, NS, B3J 3K5, Canada
byos.io/contact

4.4 - About Byos

Byos is a Network Security company based in Halifax, Nova Scotia, Canada. Our team has decades of combined experience providing defensive and offensive security solutions, on-demand incident detection and response services, personalized strategy planning and execution, and high-end, hands-on technical training for both public and private sector clients.

In 2016, we detected a problem with the way devices connect to networks, delegating security to the upper layers of software. We believe that the strongest form of device protection comes from hardware enforced network security and that's why Byos aims to become the market standard for a secure Network Interface Card (NIC), providing security without compromising connection speeds.

As the world becomes more connected, it is our mission to protect the world's most critical assets (energy platforms, biomedical devices, automobiles, ATMs, PoS systems, IoT devices, etc.) from advanced network threats.