**News Advisory:** July 22, 2015
**Topics:** Strategic Focus: Software, Products & Services

# HP Study Reveals Smartwatches Vulnerable to Attack

## HP Fortify finds 100 percent of tested smartwatches exhibit security flaws, provides guidance for secure device use

PALO ALTO, Calif., July 22, 2015 — As part of an ongoing series looking at Internet of Things (IoT) security, HP today unveiled results of an assessment confirming that smartwatches with network and communication functionality represent a new and open frontier for cyberattack. The study conducted by HP Fortify found that 100 percent of the tested smartwatches contain significant vulnerabilities, including insufficient authentication, lack of encryption and privacy concerns[1]. In the report HP provides actionable recommendations for secure smartwatch development and use, both at home and in the workplace.

As the IoT market advances, smartwatches are growing in popularity for their convenience and capabilities. As they become more mainstream, smartwatches will increasingly store more sensitive information such as health data, and through connectivity with mobile apps may soon enable physical access functions including unlocking cars and homes.

*"Smartwatches have only just started to become a part of our lives, but they deliver a new level of functionality that could potentially open the door to new threats to sensitive information and activities," said Jason Schmitt, general manager, HP Security, Fortify. "As the adoption of smartwatches accelerates, the platform will become vastly more attractive to those who would abuse that access, making it critical that we take precautions when transmitting personal data or connecting smartwatches into corporate networks."*

The HP study questions whether smartwatches are designed to store and protect the sensitive data and tasks for which they are built. HP leveraged HP Fortify on Demand to assess 10 smartwatches, along with their Android and iOS cloud and mobile application components, uncovering numerous security concerns.

The most common and easily addressable security issues reported include:

- Insufficient User Authentication/Authorization: Every smartwatch tested was paired with a mobile interface that lacked two-factor authentication and the ability to lock out accounts after 3-5 failed password attempts. Three in ten, 30 percent, were vulnerable to account harvesting, meaning an attacker could gain access to the device and data via a combination of weak password policy, lack of account lockout, and user enumeration.
- Lack of transport encryption: Transport encryption is critical given that personal information is being moved to multiple locations in the cloud. While 100 percent of the test products implemented transport encryption using SSL/TLS, 40 percent of the cloud connections continue to be vulnerable to the POODLE attack, allow the use of weak cyphers, or still used SSL v2.
- Insecure Interfaces: Thirty percent of the tested smartwatches used cloud-based web interfaces, all of which exhibited account enumeration concerns. In a separate test, 30 percent also exhibited account enumeration concerns with their mobile applications. This vulnerability enables hackers to identify valid user accounts through feedback received from reset password mechanisms.
- Insecure Software/Firmware: A full 70 percent of the smartwatches were found to have concerns with protection of firmware updates, including transmitting firmware updates without encryption and without encrypting the update files. However, many updates were signed to help prevent the installation of contaminated firmware. While malicious updates cannot be installed, lack of encryption allows the files to be downloaded and analyzed.
- Privacy Concerns: All smartwatches collected some form of personal information, such as name, address, date of birth, weight, gender, heart rate and other health information. Given the account enumeration issues and use of weak passwords on some products, exposure of this personal information is a concern.

As manufacturers work to incorporate necessary security measures into smartwatches, consumers are urged to consider security when choosing to use a smartwatch. It's recommended that users do not enable sensitive access control functions such as car or home access unless strong authorization is offered. In addition, enabling passcode functionality, ensuring strong passwords and instituting two-factor authentication will help prevent unauthorized access to data. These security measures are not only important to protecting personal data, but are critical as smartwatches are introduced to the workplace and connected to corporate networks. Additional guidelines for secure smartwatch use are outlined in the full report.

For more information, visit the first report in this IoT series, 2014 HP Internet of Things Research Study, which reviews the security of 10 of the most common IoT devices. In addition, the 2015 HP Home Security Systems Report reviews the 10 of the most common Internet-connected home security systems.

### Methodology

Conducted by HP Fortify, the HP Smartwatch Security Study used the HP Fortify on Demand IoT testing methodology which combined manual testing along with the use of automated tools. Devices and their components were assessed based on the OWASP Internet of Things Top 10 and the specific vulnerabilities associated with each top 10 category.

All data and percentages for this study were drawn from the 10 smartwatches tested during this study. While there are certainly a fair number of smartwatch devices already on the market, and that number continues to grow, HP believes the similarity in results of the 10 smartwatches provides a good indicator of the current security posture of smartwatch devices.

1 “HP Internet of Things Security Report: Smartwatches,” HP, July 2015

**About HP Security**

HP enables organizations to take a proactive approach to security, disrupting the life cycle of an attack through prevention and real-time threat detection. With market-leading products, services and innovative research, HP Enterprise Security enables organizations to integrate information correlation, application analysis and network-level defense. Additional information about HP Enterprise Security can be found at www.hp.com/go/esp.

Join HP Software on Linkedin and follow @HPSoftware on Twitter. To learn more about HP Fortify and HP Enterprise Security Products on Twitter, please follow @HPsecurity and join HP Enterprise Security on Linkedin.

HP’s annual enterprise security user conference, HP Protect, takes place September 1-4 in Washington, D.C.



This press release contains forward-looking statements that involve risks, uncertainties and assumptions. If such risks or uncertainties materialize or such assumptions prove incorrect, the results of HP and its consolidated subsidiaries could differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements, including but not limited to statements of the plans, strategies and objectives of HP for future operations, including the separation transaction; the future performance of Hewlett-Packard Enterprise and HP Inc. if the separation is completed; any statements concerning expected development, performance, market share or competitive performance relating to products and services; any statements regarding anticipated operational and financial results; any statements of expectation or belief; and any statements of assumptions underlying any of the foregoing. Risks, uncertainties and assumptions include the need to address the many challenges facing HP’s businesses; the competitive pressures faced by HP’s businesses; risks associated with executing HP’s strategy, including the planned separation transaction, and plans for future operations and investments; the impact of macroeconomic and geopolitical trends and events; the need to manage third-party suppliers and the distribution of HP’s products and services effectively; the protection of HP’s intellectual property assets, including intellectual property licensed from third parties; risks associated with HP’s international operations; the development and transition of new products and services and the enhancement of existing products and services to meet customer needs and respond to emerging technological trends; the execution and performance of contracts by HP and its suppliers, customers, clients and partners; the hiring and retention of key employees; integration and other risks associated with business combination and investment transactions; the execution, timing and results of restructuring plans, including estimates and assumptions related to the cost and the anticipated benefits of implementing those plans; the execution, timing and results of the separation transaction or restructuring plans, including estimates and assumptions related to the cost (including any possible disruption of HP’s business) and the anticipated benefits of implementing the separation transaction and restructuring plans; the resolution of pending investigations, claims and disputes; and other risks that are described in HP’s Annual Report on Form 10-K for the fiscal year ended October 31, 2015, and HP’s other filings with the Securities and Exchange Commission. HP assumes no obligation and does not intend to update these forward-looking statements.

## Media contacts

Kristi Rawlinson, HP
kristi.rawlinson@hp.com

**About HP**

HP Inc. creates technology that makes life better for everyone, everywhere. Through our portfolio of printers, PCs, mobile devices, solutions, and services, we engineer experiences that amaze. More information about HP Inc. is available at http://www.hp.com.