WILMERHALE

FTC Settles with Computer Hardware Provider Over Allegedly Flawed Router and Cloud Feature Security

FEBRUARY 24, 2016

On February 23, 2016, The Federal Trade Commission ("FTC") announced its settlement with Taiwan-based ASUSTeK Computer Inc. ("ASUS") over charges that "critical security flaws" in its routers and cloud features put the home networks and connected storage devices of consumers at risk. The FTC alleged the company was repeatedly made aware of its products' vulnerabilities, and failed to deliver readily available fixes to consumers in a timely fashion, which ultimately led to attackers gaining access to over 12,900 ASUS routers and connected storage devices in February 2014.

This enforcement action shows that the FTC is continuing to take an aggressive approach to policing data security in general, and specifically related to connected devices (IoT).

Multiple Vulnerabilities. According to the FTC complaint, both the router and the cloud features included multiple vulnerabilities that would allow attackers to gain unauthorized access to consumers' private files and login credentials. To exploit these vulnerabilities, the attacker only required the router's IP address which, according to the FTC, was "easily discoverable." In addition, the cloud feature transferred data in unencrypted text and included other serious security flaws—including multiple password vulnerabilities.

Failure to Provide Timely Notice. The FTC alleged that several consumers notified ASUS about the vulnerabilities and impact of these vulnerabilities on consumer data, as early as June 2013. Despite this knowledge, the company allegedly failed to notify consumers about the vulnerabilities, or deliver readily available fixes in a timely manner. This case illustrates once again that the FTC expects companies to pay attention to, and address, warnings from individuals and security researchers in a timely fashion.

Failure to Reasonably Secure Software. According to the complaint, ASUS failed to take reasonable steps to secure the software on its routers and related cloud features, despite its claims that the company's devices would "protect computers from any unauthorized access, hacking and virus attacks."

The complaint alleged the company did **not** take a number of "reasonable" steps, including:

- Using readily available secure protocols;
- Implementing secure default settings;
- Preventing consumers from using weak default login credentials;
- Implementing readily available, low-cost protections against well-known and reasonably foreseeable vulnerabilities;
- Maintaining an adequate process for receiving and addressing security vulnerability reports from third parties; and
- Performing vulnerability and penetration testing of the software.

Proposed Consent Terms. As has become standard practice in FTC security-related consent orders, the proposed consent order will require ASUS to establish and maintain a comprehensive security program subject to biannual, independent audits for the next 20 years. The order will also require ASUS to notify consumers about software updates or other steps they can take to protect themselves from security flaws and prohibit the company from misleading consumers about the security of the company's products.

The Internet of Things. As stated by Jessica Rich, Director of the FTC Bureau of Consumer Protection, following the ASUS settlement, "The Internet of Things is growing by leaps and bounds, with millions of consumers connecting smart devices to their home networks." This is the second data security case by the FTC involving the "Internet of Things"—with signs there are more to come. As the number of devices in the home connected to the Internet increase exponentially, so do the data security risks.