
black hat
USA 2017
JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS
Firmware is the new Black – Analyzing Past 3 years of BIOS/UEFI Security Vulnerabilities
Bruce Monroe & Rodrigo Rubira Branco (@bsdaemon) & Vincent Zimmer (@vincentzimmer)
{ bruce.monroe || rodrigo.branco || vincent.zimmer } @ intel.com
#BHUSA / @BLACKHATEVENTS

Abstract

- In recent years we witnessed the rise of firmware-related vulnerabilities, likely a direct result of increasing adoption of exploit mitigations in major/widespread operating systems, including for mobile phones. Pairing that with the recent (and not so recent) leaks of government offensive capabilities abusing supply chains and using physical possession to persist on compromised systems, it is clear that firmware is the new black in security. This research looks into BIOS/UEFI platform firmware, trying to help making sense of the threat. We present a threat model, discuss new mitigations that could have prevented the issues and offer a categorization of bug classes that hopefully will help focusing investments in protecting systems (and finding new vulnerabilities). Our data set comprises of 90+ security vulnerabilities handled by Intel Product Security Incident Response Team (PSIRT) in the past 3 years and the analysis was manually performed, using white-box and counting with feedback from various BIOS developers within the company (and security researchers externally that reported some of the issues - most of the issues were found by internal teams, but PSIRT is involved since they were found to also affect released products).

Latest Version

- The latest version of this material can be obtained at:
  https://github.com/rrbranco/BlackHat2017

- Give us at least a day after the presentation in Black Hat

Acknowledgements

- Lots of different individuals (and teams) inside and outside of Intel contribute to the evolution of UEFI security

- Without them, this talk would not have been possible and we strongly appreciate their help, continuous feedback and work

QUESTIONS?

Bruce Monroe & Rodrigo Rubira Branco (@bsdaemon) & Vincent Zimmer (@vincentzimmer)
{ bruce.monroe || rodrigo.branco || vincent.zimmer } @ intel.com