PixieFail UEFI Flaws Expose Millions of Computers to RCE, DoS, and Data Theft

The Hacker News ⋮ 3-4 minutes

Firmware Security / Vulnerability

Multiple security vulnerabilities have been disclosed in the TCP/IP network protocol stack of an open-source reference implementation of the Unified Extensible Firmware Interface (UEFI) specification used widely in modern computers.

Collectively dubbed **PixieFail** by Quarkslab, the nine issues reside in the TianoCore EFI Development Kit II (EDK II) and could be exploited to achieve remote code execution, denial-of-service (DoS), DNS cache poisoning, and leakage of sensitive information.

UEFI firmware – which is responsible for booting the operating system – from AMI, Intel, Insyde, and Phoenix Technologies are impacted by the shortcomings.

EDK II incorporates its own TCP/IP stack called NetworkPkg to enable network functionalities available during the initial Preboot eXecution Environment (PXE, pronounced "pixie") stage, which allows for management tasks in the absence of a running operating system.

In other words, it is a client-server interface to boot a device from its network interface card (NIC) and allows networked computers that are not yet loaded with an operating system to be configured and booted remotely by an administrator.

The code to PXE is included as part of the UEFI firmware on the motherboard or within the NIC firmware read-only memory (ROM).

The issues identified by Quarkslab within the EDKII's NetworkPkg encompass overflow bugs, out-of-bounds read, infinite loops, and the use of weak pseudorandom number generator (PRNG) that result in DNS and DHCP poisoning attacks, information leakage, denial of service, and data insertion attacks at the IPv4 and IPv6 layer.

The list of flaws is as follows -

- **CVE-2023-45229** (CVSS score: 6.5) - Integer underflow when processing IA_NA/IA_TA options in a DHCPv6 Advertise message
- **CVE-2023-45230** (CVSS score: 8.3) - Buffer overflow in the DHCPv6 client via a long Server ID option
- **CVE-2023-45231** (CVSS score: 6.5) - Out-of-bounds read when handling a ND Redirect message with truncated options
- **CVE-2023-45232** (CVSS score: 7.5) - Infinite loop when parsing unknown options in the Destination Options header
- **CVE-2023-45233** (CVSS score: 7.5) - Infinite loop when parsing a PadN option in the Destination Options header
- **CVE-2023-45234** (CVSS score: 8.3) - Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message
- **CVE-2023-45235** (CVSS score: 8.3) - Buffer overflow when handling Server ID option from a DHCPv6 proxy Advertise message
- **CVE-2023-45236** (CVSS score: 5.8) - Predictable TCP Initial Sequence Numbers
- **CVE-2023-45237** (CVSS score: 5.3) - Use of a weak pseudorandom number generator

"The impact and exploitability of these vulnerabilities depend on the specific firmware build and the default PXE boot configuration," the CERT Coordination Center (CERT/CC) said in an advisory.

"An attacker within the local network (and, in certain scenarios remotely) could exploit these weaknesses to execute remote code, initiate DoS attacks, conduct DNS cache poisoning, or extract sensitive information."

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.