Critical Boot Loader Vulnerability in Shim Impacts Nearly All Linux Distros

Feb 07, 2024 Newsroom

The maintainers of shim have released version 15.8 to address six security flaws, including a critical bug that could pave the way for remote code execution under specific circumstances.

Tracked as **CVE-2023-40547** (CVSS score: 9.8), the vulnerability could be exploited to achieve a Secure Boot bypass. Bill Demirkapi of the Microsoft Security Response Center (MSRC) has been credited with discovering and reporting the bug.

Major Linux distributions that use shim such as Debian, Red Hat, SUSE, and Ubuntu have all released advisories for the security flaw.

"The shim's http boot support (httpboot.c) trusts attacker-controlled values when parsing an HTTP response, leading to a completely controlled out-of-bounds write primitive," Oracle's Alan Coopersmith noted in a message shared on the Open Source Security mailing list oss-security.

Demirkapi, in a post shared on X (formerly Twitter) late last month, said the vulnerability "exists in every Linux boot loader signed in the past decade."

shim refers to a "trivial" software package that's designed to work as a first-stage boot loader on Unified Extensible Firmware Interface (UEFI) systems.

Firmware security firm Eclypsium said CVE-2023-40547 "stems from HTTP protocol handling, leading to an out-of-bounds write that can lead to complete system compromise."

In a hypothetical attack scenario, a threat actor on the same network could leverage the flaw to load a vulnerable shim boot loader, or by a local adversary with adequate privileges to manipulate data on the EFI partition.

"An attacker could perform a MiTM (Man-in-the-Middle) attack and intercept HTTP traffic between the victim and the HTTP server used to serve files to support HTTP boot," the company added. "The attacker could be located on any network segment between the victim and the legitimate server."

That said, obtaining the ability to execute code during the boot process – which occurs before the main operating system starts – grants the attacker carte blanche access to deploy stealthy bootkits that can give near-total control over the compromised host.

The five other vulnerabilities fixed in shim version 15.8 are below -

- CVE-2023-40546 (CVSS score: 5.3) - Out-of-bounds read when printing error messages, resulting in a denial-of-service (DoS) condition
- CVE-2023-40548 (CVSS score: 7.4) - Buffer overflow in shim when compiled for 32-bit processors that can lead to a crash or data integrity issues during the boot phase
- CVE-2023-40549 (CVSS score: 5.5) - Out-of-bounds read in the authenticode function that could permit an attacker to trigger a DoS by providing a malformed binary
- CVE-2023-40550 (CVSS score: 5.5) - Out-of-bounds read when validating Secure Boot Advanced Targeting (SBAT) information that could result in information disclosure
- CVE-2023-40551 (CVSS score: 7.1) - Out-of-bounds read when parsing MZ binaries, leading to a crash or possible exposure of sensitive data

"An attacker exploiting this vulnerability gains control of the system before the kernel is loaded, which means they have privileged access and the ability to circumvent any controls implemented by the kernel and operating system," Eclypsium noted.