ESET Research discovers vulnerable UEFI shims undermining devices' Secure Boot

DUBAI , DUBAI, UNITED ARAB EMIRATES, July 23, 2026 /EINPresswire.com/ -- ESET researchers discovered 11 vulnerable UEFI shim bootloaders signed by Microsoft that allow attackers to bypass UEFI Secure Boot by exploiting decade-old vulnerabilities. UEFI shim bootloaders are tiny bits of code designed to bridge the gap between motherboard UEFI firmware and an operating system. The vulnerable shims, at versions 0.9 and below, can be used to bypass UEFI Secure Boot on any UEFI-based machine that trusts the Microsoft Corporation UEFI CA 2011 third-party UEFI certificate authority (CA) certificate, regardless of the installed operating system. Reported shims can be exploited to execute untrusted code during system boot, enabling attackers to deploy malicious UEFI bootkits even on systems with UEFI Secure Boot enabled. ESET reported findings to CERT/CC; the vulnerable UEFI applications were then revoked.

The discovered shims come from various tools or software packages, including PC-diagnostic software, Linux distributions, and other UEFI-based utilities. Importantly, exploitation is not limited to systems with the affected software or OS installed, as attackers can bring their own copy of the vulnerable shims to any UEFI system with the Microsoft third-party UEFI certificate enrolled.

"What makes these old shims dangerous is not a novel vulnerability; it's that no new vulnerability is needed to bypass UEFI Secure Boot. An attacker needs no complicated exploitation primitives – only a copy of an old, still-trusted, but unrevoked shim binary and a basic understanding of how UEFI shims work. That is enough to bypass such an essential security feature as UEFI Secure Boot," says ESET researcher Martin Smolár, who discovered the vulnerable shims.

"To understand the impact that such vulnerable shims can have on UEFI Secure Boot-protected systems, in the report we examine a few specific issues in the reported shims – issues that are easily exploitable and that highlight the breadth of the attack surface they expose," adds

Smolár.

Over the years, the UEFI shim bootloader has naturally evolved, with new improvements and security features introduced in successive releases of the upstream UEFI shim repository. At the same time, many third-party vendors have taken available versions of the shim source code to build their own binaries, which they subsequently submitted to Microsoft for signing. This behavior is expected and aligns with the original design of shims. However, insufficient attention has been given to revoking outdated Microsoft-signed shims, many of which can, by design, be leveraged to bypass newer security mechanisms.

These vulnerable shims can be blocked by applying the latest UEFI revocations from Microsoft. Windows systems should be updated automatically. For Linux systems, updates should be available through the Linux Vendor Firmware Service. For more general recommendations regarding how to protect against (or at least detect) exploitation of unknown vulnerable signed UEFI bootloaders and deployment of UEFI bootkits, see ESET Research blogpost: Under the cloak of UEFI Secure Boot: Introducing CVE-2024-7344.

For a more details about the vulnerable UEFI shims, check out the ESET Research blogpost “Forgotten UEFI shims undermining Secure Boot" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it’s endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts, and blogs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.