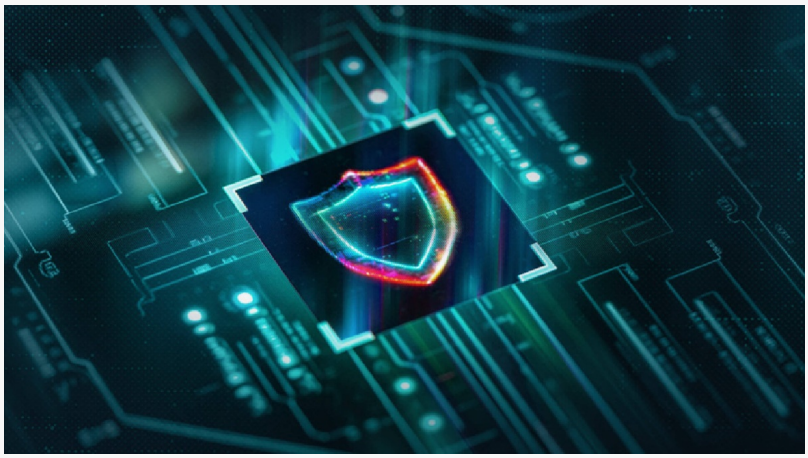
ESET Research discovers UEFI Secure Boot bypass vulnerability



DUBAI , DUBAI, UNITED ARAB EMIRATES, January 20, 2025 /EINPresswire.com/ -- ESET researchers have discovered a vulnerability, affecting the majority of UEFI-based systems, that allows actors to bypass UEFI Secure Boot. This vulnerability, assigned CVE-2024-7344, was found in a UEFI application signed by Microsoft's "Microsoft Corporation UEFI CA 2011" third-party UEFI certificate. Exploitation of this vulnerability can lead to the execution of untrusted code during system boot, enabling potential attackers to easily deploy malicious UEFI bootkits (such as Bootkitty or BlackLotus) even on systems with UEFI Secure Boot enabled, regardless of the operating system installed.

ESET reported the findings to the CERT Coordination Center (CERT/CC) in June 2024, which successfully contacted the affected vendors. The issue has now been fixed in affected products, and the old, vulnerable binaries were revoked by Microsoft in the January 14, 2025, Patch Tuesday update.

The affected UEFI application is part of several real-time system recovery software suites developed by Howyar Technologies Inc., Greenware Technologies, Radix Technologies Ltd., SANFONG Inc., Wasay Software Technology Inc., Computer Education System Inc., and Signal Computer GmbH.

"The number of UEFI vulnerabilities discovered in recent years and the failures in patching them or revoking vulnerable binaries within a reasonable time window shows that even such an essential feature as UEFI Secure Boot should not be considered an impenetrable barrier," says ESET researcher Martin Smolár, who discovered the vulnerability. "However, what concerns us the most with respect to the vulnerability is not the time it took to fix and revoke the binary, which was quite good compared to similar cases, but the fact that this isn't the first time that such an obviously unsafe signed UEFI binary has been discovered. This raises questions of how

common the use of such unsafe techniques is among third-party UEFI software vendors, and how many other similar obscure, but signed, bootloaders there might be out there."

Exploitation of this vulnerability is not limited to systems with the affected recovery software installed, as attackers can bring their own copy of the vulnerable binary to any UEFI system with the Microsoft third-party UEFI certificate enrolled. Also, elevated privileges are required to deploy the vulnerable and malicious files to the EFI system partition (local administrator on Windows; root on Linux). The vulnerability is caused by the use of a custom PE loader instead of using the standard and secure UEFI functions LoadImage and StartImage. All UEFI systems with Microsoft third-party UEFI signing enabled are affected (Windows 11 Secured-core PCs should have this option disabled by default).

The vulnerability can be mitigated by applying the latest UEFI revocations from Microsoft. Windows systems should be updated automatically. Microsoft's advisory for the CVE-2024-7344 vulnerability can be found here. For Linux systems, updates should be available through the Linux Vendor Firmware Service.

For a more detailed analysis and technical breakdown of the UEFI vulnerability, check out the latest ESET Research blogpost "Under the cloak of UEFI Secure Boot: Introducing CVE-2024-7344" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of known and emerging cyberthreats — 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. An 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 us on LinkedIn, Facebook, and X.

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