# Yet Another EFI/UEFI Exploit, this one Utilizing NVRAM and Persistent Storage – Purism

2-2 minutes ⋮ 3/27/2017

- About
- Latest Posts

## Todd Weaver

Founder and CEO
PGP Fingerprint: B8CA ACEA D949 30F1 23C4 642C 23CF 2E3D 2545 14F7

Continuing on our previous post on this topic, another EFI/UEFI BIOS exploit theoretically known–and even proven to work by Trammel hudson some years ago–that resurfaced through the Vault 7 documents, is the EFI/UEFI exploit that can write to NVRAM or persistent storage. This means that this exploit **cannot be detected from hard drive inspection,** and **can survive through a complete OS reinstall if you're using EFI/UEFI** (which is not a problem for Purism users running coreboot).

The CIA documents describe it best:

> "These variables present interesting opportunities for our tools since they will survive a OS reinstall and are invisible to a forensic image of the hard drive. What's also interesting is that there is no way to enumerate NVRAM variables from the OS… you have to know the exact GUID and name of the variable to even determine that it exists." — the CIA, as leaked through the Vault 7 Persistent Storage Document

This line also summarizes intent for the exploit:

> "This might be a good place to put either implants or encryption keys. If every implant deployment used a different GUID/name pair, it would make the variables a bit more difficult to discover." — the CIA, from the Vault 7 Persistent Storage Document

This continues to reinforce that our philosophy and beliefs are the only way to have long-term products that respects users' digital rights.