ESCALATING INSIDER THREATS USING VMWARE'S API

Ofri Ziv, GuardiCore
Who am I?

• VP Research at GuardiCore
  • Head of GuardiCore Labs
  • Security research
  • Development of data analysis algorithms
• Msc in Computer Science
• Over 10 years of cyber security research experience
• Prior work: Bondnet, Infection Monkey

GuardiCore

• Cloud & Data Center security company
• www.guardicore.com
Agenda

• Overview of host-guest isolation model

• Use case (SOD)

• Attack Flow

• Demo

• Who is vulnerable?

• Mitigation
From vSphere User to Guest Machine RCE
Host-Guest Isolation

- Any virtualized data center needs to provide isolation between host and guest machines
- Separation of Duties
- Required by regulations
Host-Guest Isolation

"Guest virtual machines should be isolated from the host and from other guests running on the same host. Interaction between the host and guests [...] should occur only through channels with well-understood and documented security properties."

- VMware

Isolation – How To

“

To use the VIX API for guest operation, applications must authenticate with two distinct security domains:
1. The client must first authenticate with the vSphere host.
2. The client must then supply a valid credential for the guest operating system on any virtual machine where it wants to perform guest operations

- VMware


”
A built-in functionality in vSphere breaks the host-guest security model.
Escalating Insider Threats Using VMware’s API

Patients Data

Dr. Bob

Alice
Escalating Insider Threats Using VMware’s API

Dr. Bob

Patients Data

Host Cred

Guest Cred

Alice

Host Cred

Guest Cred

HOST

DATA PLANE

CONTROL PLANE

GUEST

Patients Data

HOST

DATA PLANE

CONTROL PLANE
Escalating Insider Threats Using VMware’s API

Dr. Bob

Patients Data

CONTROL PLANE

DATA PLANE

Host Cred

Guest Cred

GUEST

HOST

Alice

Host Cred

Guest Cred

Patients Data

GUEST

HOST
Escalating Insider Threats Using VMware’s API

Dr. Bob

Host Cred

Guest Cred

Alice

Host Cred

Guest Cred

DATA PLANE

CONTROL PLANE

Patients Data
Escalating Insider Threats Using VMware’s API

**DATA PLANE**

**CONTROL PLANE**

- Host Cred
- Guest Cred
  - Dr. Bob
  - Alice

- Patients Data

---

Dr. Bob

Patients Data

---

Host Cred

Guest Cred

---

Alice

---
Escalating Insider Threats Using VMware’s API

Dr. Bob

Patients Data

HOST

GUEST

DATA PLANE

CONTROL PLANE

Host Cred

Guest Cred

Alice

Host Cred

Guest Cred
An undocumented feature

- Undocumented authentication method
- Bypass guest authentication
- Leads to RCE on the guest machine
Broken Host-Guest Isolation

"To use the VIX API for guest operation, applications must authenticate with two distinct security domains:

1. The client must first authenticate with the vSphere host.
2. The client must then supply a valid credential for the guest operation—system on any virtual machine where it wants to perform guest operations."

- VMware

All your GUEST are belong to us

• Control the guest
  • Arbitrary code execution
  • File operations
  • Registry operations

• Attack types
  • Lateral Movement
  • Access to isolated networks
  • Data leakage / manipulation
  • Ransomware
What does the diagram illustrate about the data flow and security measures in a VMware environment?
**Undocumented Authentication Method**

**Name**

VixVM_LoginInGuest

**Description**

VixHandle

VixVM_LoginInGuest(VixHandle vmHandle,
    char *userName,
    char *password,
    int options,
    VixEventProc *callbackProc,
    void *clientData);

This function establishes a guest operating system authentication context that can be used with guest functions for the given virtual machine handle.

**Parameters**

*vmHandle*
Identifies a virtual machine. Call VixVM_Open() to create a virtual machine handle.

*userName*
The name of a user account on the guest operating system.

*password*
The password of the account identified by userName.

*options*

Must be 0 or VIX_LOGIN_IN_GUEST_REQUIRE_INTERACTIVE_ENVIRONMENT, which forces interactive guest login within a graphical session that is visible to the user (see below). On Linux, interactive environment requires that the X11 window system be running to start the VMware-user process. Without X11, pass 0 as options to start the vmware-guestos process instead.

*callbackProc*
A callback function that will be invoked when the operation is complete.

*clientData*
A parameter that will be passed to the callbackProc function.
Connect (host cred)
Vix_OpenVm ("Patients Data")
LoginInGuest(Shared Secret User,
Shared Secret, options=4)
How to Set a Shared Secret

- Shared Secret Login
  - vSphere API
  - “VirtualMachine\Config\AdvancedConfig” privilege

```
guest.commands.sharedSecretLogin.<USERNAME> = SHA256(SS).encode(“base64”)
```

```
~ # cat /vmfs/....confidential_vm.vmx
replay.filename = ""
scsi0:0.redo = ""
vmci0.id = "-201902441"
cleanShutdown = "FALSE"
toolsInstallManager.updateCounter = "10"
guest.commands.sharedSecretLogin.com.guardicore.VIX_DEMO = "1T7aemN8mcx/tWbZbp+hCb8VxHhBCi9etNTE4mzOgfY=
```
How to Set a Shared Secret

• Shared Secret Login
  • vSphere API
  • “VirtualMachine\Config\AdvancedConfig” privilege

  guest.commands.sharedSecretLogin.<USERNAME> = SHA256(SS).encode(“base64”)

• SharedPolicyRefCount
  • Controls whether guest operations using shared secret are allowed
  • vSphere API
  • “Host\Configuration\Advanced Settings” privilege
Connect (host cred) Vix_OpenVm (“Patients Data”) LoginInGuest(Shared Secret User, Shared Secret, options=4) RunProgramInGuest(“/bin/sh”)

Attack Flow
Attack Flow

Connect (host cred) Vix_OpenVm (“Patients Data”)
LoginInGuest(Shared Secret User, Shared Secret, options=4)
RunProgramInGuest(“/bin/sh”)
Connect (host cred)
Vix_OpenVm (“Patients Data”)
LoginInGuest(Shared Secret User,
Shared Secret, options=4)
RunProgramInGuest(“/bin/sh”)
Live DEMO!
When will the attack not work?

```c

case VIX_USER_CREDENTIAL_ROOT:
{
    if (!(requestMsg->requestFlags & VIX_REQUESTMSG_HAS_HASHED_SHARED_SECRET) &&
        !VixToolsCheckIfAuthenticationTypeEnabled(gConfDictRef,
        VIX_TOOLS_CONFIG_AUTHTYPE_AGENTS)) {
        g_message("%s: Requested authentication type has been disabled.\n", __FUNCTION__);
        err = VIX_E_GUEST_AUTHTYPE_DISABLED;
        goto done;
    }

    // fall through

    case VIX_USER_CREDENTIAL_CONSOLE_USER:
    err = VixToolsImpersonateUserImplEx(NULL,
    credentialType,
    NULL,
    userToken);
```

Who is vulnerable?

- Guest machines running on ESXi 5.5

OR

- Guest machines running VMware Tools version < 10.1.0

- Latest upstream repository offers a vulnerable OVT
  - Ubuntu 16.10
  - Fedora 25
  - RHEL 7.2
  - Oracle Linux 7 (latest)
Our Risk Assessment Tool

https://github.com/guardicore/vmware_guest_auth_bypass
Mitigation

• For ESXi 6.0 and 6.5
  • Option #1 – Upgrade Vmtools ≥ 10.1.0
  • Option #2 – Opt-out by modifying vmtools configuration (for ≥ 9.9.0)

```bash
[guestoperations]
Authentication.InfrastructureAgents.disabled = True
```
Mitigation

• For ESXi 5.5
  • Fixed VMtools version
    • Forked from latest open-vm-tools repository
    • Source code - https://github.com/guardicore/open_vm_tools
  • Binary
Go Check your network

https://github.com/guardicore/vmware_guest_auth_bypass
  • Attack tool
  • Risk assessment tool

Fixed vmtools version
  • Source: https://github.com/guardicore/open_vm_tools
  • Binary

ofri@guardicore.com

@OfriZiv (twitter)