

Tech Zone

- [VMware by Broadcom 보안 권고 발행: VMSA-2024-0006](#)

VMware by Broadcom 보안 권고

발행: VMSA-2024-0006

소개

2024년 3월 5일, Broadcom은 VMware ESXi, VMware Workstation Pro & Player, VMware Fusion에서 발견된 보안 취약성을 다루는 보안 권고 사항인 VMSA-2024-0006을 발표했습니다. 이 권고 사항은 데스크톱 제품에는 "심각(Critical)" 수준이지만, vSphere 7 이후 ESXi에 존재하는 보안 조치로 인해 VMware ESXi에는 "중요(important)" 수준입니다.

따라서 해당 제품을 패치하는 것이 문제를 해결하는 가장 빠른 방법입니다. 환경에 따라 가상 머신에서 USB 컨트롤러를 제거하여 해결 방법을 사용할 수 있습니다. 그러나 이 방법은 대규모로 실행하기 어려울 수 있으며 가상 머신 콘솔 액세스에 영향을 줄 수 있습니다. 자세한 내용은 아래 Q&A를 참조하십시오.

영향을 받는 제품 및 버전, 해결 방법, 조직의 보안을 유지하는 데 필요한 적절한 패치에 관한 정보는 VMware Security Advisory (VMSA)에서 확인할 수 있습니다. 이 문서는 이 권고에 대한 보조 가이드 역할을 하며, 사용자와 조직이 적절한 대응을 결정하는 데 도움이 되는 셀프 서비스 정보를 제공합니다.

현재 업데이트

2024년 3월 5일 2000 PST(-0800)에 업데이트되었습니다.

다음 예상 업데이트

이 문서에는 정기적인 업데이트 일정이 없습니다.

연결

[VMware 보안 권고 VMSA-2024-0006 \(문제 설명\)](#)

[vSphere 보안 구성 및 강화 가이드](#) (VMware vSphere, 가상 머신 및 VMware Tools와 같은 게스트 내 설정 강화에 대한 참조)

[VMware 보안 권고](#) (공개된 모든 보안 취약점 목록)

[VMware 보안 권고 메일링 목록](#) (보안 권고에 대한 사전 알림을 받기 위한 구독 신청)

[VMware vSphere 패치 모범 사례](#) (패치 성공을 위한 안내)

질문과 답변

누구에게 영향을 미치나요?

VMware Workstation, VMware Fusion 및/또는 VMware ESXi를 단독으로 또는 VMware vSphere 또는 VMware Cloud Foundation의 일부로 배포한 고객에게 영향을 미칩니다.

언제 조치를 취해야 합니까?

ITIL 측면에서 이 상황은 긴급 변경 사항에 해당하므로 조직에서 즉각적인 조치가 필요합니다. 그러나 적절한 보안 대응은 구체적인 상황에 따라 달라질 수 있습니다. 조직의 정보 보안 담당자와 상의하여 조직의 필요에 맞는 최선의 조치를 결정하는 것이 중요합니다.

어떻게 보호할 수 있나요?

해당되는 제품을 VMSA에 나열된 버전 이상으로 업데이트하여 자신과 조직을 보호할 수 있습니다.

어떤 제품이 영향을 받나요?

VMSA에는 영향을 받는 지원되는 모든 제품과 버전이 나열되어 있습니다.

vSphere 6.x가 영향을 받나요?

예. 일반 지원 기간이 끝난 모든 소프트웨어 제품은 위험에 처해 있는 것으로 간주되어야 합니다. 가능한 신속히 vSphere 7 또는 8로 업그레이드하시기 바랍니다.

ESXi 6.7, 6.5 또는 VMware Cloud Foundation 3.x에 대한 확장 지원 계약이 있는 경우 VMSA의 지침에 따라 업데이트를 확인하십시오.

해당 공지와 관련된 CVE 번호는 무엇입니까?

CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255.

이 VMSA에 공개된 취약점의 심각도는 무엇입니까?

VMware 보안 권고는 CVSS(Common Vulnerability Scoring Standard) 버전 3.1을 사용하여 심각도를 결정합니다. 구체적인 점수는 VMSA 문서를 참조하십시오.

개별 취약점의 벡터에 대한 자세한 정보가 있습니까?

예, VMware 보안 권고에서는 각 개별 취약점에 대한 벡터가 미리 입력된 FIRST CVSS v3.1 계산기 링크를 제공합니다. 이 정보는 보안 권고의 '참조' 섹션에서 확인할 수 있습니다.

공개된 취약점이 "실제 환경"에서 악용되고 있습니까?

현재로서는 VMware는 이러한 취약점이 "실제 환경" 악용된 사례를 인지하지 못했습니다. 이러한 상황이 변경되면 VMSA 및 해당 문서도 이에 따라 업데이트 됩니다. 사전 경고를 받으려면 VMSA 메일링 리스트를 구독하세요.

VMware vCenter Server를 패치해야 합니까?

vCenter Server는 이 VMSA의 직접적인 영향을 받지 않습니다. Broadcom에서는 vCenter Server를 ESXi 버전과 동기화된 상태로 유지할 것을 적극 권장합니다.

VMware ESXi를 패치해야 합니까?

예. ESXi는 이 VMSA의 영향을 받습니다.

VMware Cloud Foundation을 패치해야 합니까?

예. VMware Cloud Foundation은 이 VMSA의 영향을 받습니다.

영향을 받는 제품을 패치를 적용하는 대신 방화벽으로 차단할 수 있습니까?

모든 조직은 서로 다른 환경과 요구 사항을 가지고 있습니다. 이러한 상황에서 방화벽이 적합한 보완 제어 수단인지 여부는 사용자와 정보 보안 담당자가 평가해야 합니다. 특별한 경우, 워크로드에 대한 관리자/루트 수준의 액세스 권한이 있는 모든 사람이 취약점을 악용할 수 있습니다.

ESXi 취약점이 중요 취약점으로 나열되지 않은 이유는 무엇입니까?

가상 머신에 대한 로컬 관리 권한이 있는 악의적인 공격자는 이 문제를 악용하여 호스트에서 실행 중인 가상 머신의 VMX 프로세스로서 코드를 실행할 수 있습니다. ESXi 7 이상에서는 이 익스플로잇이 VMX 샌드박스 내에 포함되는

반면, Workstation 및 Fusion에서는 Workstation 또는 Fusion이 설치된 머신에서 코드 실행으로 이어질 수 있습니다.

이러한 취약점에 대한 해결 방법이 있습니까?

가상 머신 콘솔 기능에 영향을 줄 수 있는 USB 컨트롤러를 VM에서 제거할 수 있습니다. 각 조직은 자신의 환경에 맞게 이러한 조치를 효과적으로 구성하는 방법을 스스로 평가해야 합니다. 해결 방법은 복잡성을 유발하고 근본적인 문제를 해결하지 못하므로 Broadcom은 취약점을 제거하기 위해 패치를 적용할 것을 강력히 권장합니다.

해결 방법을 사용하면 단점이 있습니까?

나열된 해결 방법은 가상 머신에서 USB 컨트롤러를 제거해야 합니다. 이 방법은 대규모로 실행하기 어려울 수 있으며 일부 지원되는 운영 체제에서는 가상 콘솔을 통한 키보드 및 마우스 액세스를 위해 USB가 필요합니다(vCenter Server 또는 ESXi를 통해 가능하지만 원격 데스크톱에는 영향을 미치지 않음). 또한 USB 패스스루와 같은 일부 기능이 손실될 수도 있습니다.

하지만 대부분의 Windows 및 Linux 버전은 가상 PS/2 마우스 및 키보드 사용을 지원하며, VMware가 게시하는 보안 강화 지침의 일부로 USB 컨트롤러와 같은 불필요한 기기를 제거할 것을 권장합니다.

내 가상 머신에 USB 컨트롤러가 연결되어 있는지 어떻게 확인할 수 있습니까?

vSphere Client UI를 사용하는 것 외에도 PowerCLI를 사용하여 USB 및 기타 디바이스에 대한 감사를 수행할 수 있습니다:

```
$VMs = Get-VM
$USBHardware = "VirtualUSBController|VirtualUSBXHCIController"
foreach ($VM in $VMs) {
    $VMview = Get-VM $VM | Get-View
    $VMview.Config.Hardware.Device | Where-Object {$_.GetType().Name -match $USBHardware} | Foreach-Object {
        $devname = $_.GetType().Name
        Write-Host "$VM`: VM has a $devname device." -ForegroundColor Yellow
    }
}
```

(잠재적으로 불필요한 가상 하드웨어를 감사하는 경우 더 많은 목록이 포함될 수 있습니다. :

"VirtualUSBController|VirtualUSBXHCIController|VirtualParallelPort|VirtualFloppy|VirtualSerialPort|VirtualHdAudioCard|VirtualEnsoniq1371|VirtualCdrom|VirtualAHCIController")

PowerCLI를 사용하여 USB 컨트롤러를 제거할 수 있습니까?

예. 게스트 운영 체제 및 hot-add/hot-remove 에 대한 장치 지원에 따라 가상 머신의 전원을 꺼야 할 수도 있습니다.

```

$VMs = Get-VM $vmname
$USBHardware = "VirtualUSBController|VirtualUSBXHCIController"
foreach ($VM in $VMs) {
    $VMview = Get-VM $VM | Get-View
    $VMview.Config.Hardware.Device | Where-Object {$_.GetType().Name -match $USBHardware} | Foreach-Object {
        $devname = $_.GetType().Name
        Write-Host "$VM`: Removing the $devname device." -ForegroundColor Yellow
        $Config = New-Object VMware.Vim.VirtualMachineConfigSpec
        $Config.DeviceChange = New-Object VMware.Vim.VirtualDeviceConfigSpec
        $Config.DeviceChange[0] = New-Object VMware.Vim.VirtualDeviceConfigSpec
        $Config.DeviceChange[0].Operation = "remove"
        $Config.DeviceChange[0].Device = $_
        # $VM.ExtensionData.ReconfigVM($Config)
    }
}

```

\$vmname 변수에 값을 바꾸거나 할당하고 실제로 변경하려면 ReconfigVM 행의 주석 처리를 제거합니다. (안전을 위해 여기에 주석 처리되어 있습니다). 또한 위의 더 긴 하드웨어 목록과 함께 사용하도록 설정되었습니다 (종속성으로 인해 AHCI 컨트롤러를 제거하려면 두 번 실행해야 할 수도 있음). 또한 \$vmname을 모두 제거하면 환경의 모든 가상 머신에 대해 반복할 수 있습니다 (위험합니다!).

모든 코드 샘플과 마찬가지로 작업을 자동화하고자 하는 고객을 지원하기 위해 제공합니다. 그러나 모든 환경은 다르므로 VMware는 이 코드 샘플이 사용자 환경에 미치는 영향에 대해 책임을 지지 않습니다. 통제된 환경에서 테스트하고, 프로덕션 환경에서 사용하기 전에 영향을 이해하고, 이러한 변경을 수행할 수 있는 적절한 권한을 획득하고, 변경을 수행하기 전에 조직에 변경 사항을 전달했는지 확인하십시오.

또한 스냅샷은 가상 머신 구성을 캡처하므로 테스트 또는 이러한 변경으로 인한 위험을 완화하기 위해 가상 머신의 스냅샷을 생성할 수 있습니다. 또한 가상 머신의 스냅샷에는 USB 컨트롤러가 포함될 수 있으므로 이를 되돌리면 다시 취약해질 수 있습니다. 그렇기 때문에 취약점을 완전히 제거할 수 있는 ESXi 패치가 환경 보안을 위한 최선의 방법으로 항상 권장됩니다. 스냅샷을 생성하는 경우 장기 스냅샷에서 발생할 수 있는 일반적인 성능 및 용량 문제를 피하기 위해 적시에 스냅샷을 제거해야 합니다.

변경 로그

2024-03-05, 0800 PST(-0800): 최초 게시.

2024-03-05, 2000 PST(-0800): ESXi 6.5, 6.7 및 VCF 3.x에 대해 확장 지원 패치를 사용할 수 있음을 나타내기 위해 업데이트되었습니다.

부인 성명

이 문서는 Broadcom 솔루션을 고려하는 조직에 일반적인 지침을 제공하기 위해 작성되었습니다. 이 문서에 포함된 정보는 교육 및 정보 제공의 목적으로만 제공됩니다. 이 문서는 조언을 제공하기 위한 것이 아니며 "있는 그대로" 제공됩니다. Broadcom은 여기에 포함된 정보의 정확성, 완전성 또는 적절성에 대해 어떠한 주장, 약속 또는 보증도 하지 않습니다. 조직은 요구 사항 및 구현 효과를 검토하기 위해 특정 조직 내에서 적절한 법률, 비즈니스, 기술 및 감사 전문 지식을 활용해야 합니다.

출처 : <https://core.vmware.com/resource/vmsa-2024-0006-questions-answers#links>