



Abstract –this document provides a comprehensive analysis of CVE-2024-21111, a critical vulnerability in Oracle VM VirtualBox affecting Windows hosts. The analysis will cover various aspects of the vulnerability, including its technical details, exploitation mechanisms, potential impacts on different industries.

This document provides a high-quality summary of the vulnerability, offering valuable insights for security professionals and other stakeholders across various industries. The analysis is beneficial for understanding the risks associated with CVE-2024-21111 and implementing effective measures to safeguard systems against potential attacks.

I. INTRODUCTION

CVE-2024-21111 is a significant security vulnerability identified in Oracle VM VirtualBox, specifically affecting Windows hosts. This vulnerability is present in versions of VirtualBox prior to 7.0.16. It allows a low privileged attacker with logon access to the infrastructure where Oracle VM VirtualBox is executed to potentially take over the system.

An attacker exploiting this vulnerability could achieve unauthorized control over the affected Oracle VM VirtualBox. The specific technical mechanism involves local privilege escalation through symbolic link following, which can lead to arbitrary file deletion and movement.

II. TECHNICAL DETAILS

- **Vulnerability Type:** Local Privilege Escalation (LPE) allows a low privileged attacker who already has access to the system to gain higher privileges.
- **Attack Vector and Complexity:** The CVSS 3.1 vector (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) indicates that the attack vector is local (AV:L), meaning the attacker needs local access to the host. The attack complexity is low (AC:L), and no user interaction (UI:N) is required. The privileges required are low (PR:L), suggesting that an attacker with basic user privileges can exploit this vulnerability.

- **Impact:** The impacts on confidentiality, integrity, and availability are all rated high (C:H/I:H/A:H), indicating that an exploit could lead to a complete compromise of the affected system's confidentiality, integrity, and availability.
- **Exploitation Method:** The vulnerability can be exploited through symbolic link (symlink) attacks. This involves manipulating symbolic links to redirect operations intended for legitimate files or directories to other targets, which the attacker controls. This can lead to arbitrary file deletion or movement, potentially allowing the attacker to execute arbitrary code with elevated privileges.
- **Specific Mechanism:** The vulnerability specifically involves the manipulation of log files by the VirtualBox system service (VboxSDS). The service, which runs with SYSTEM privileges, manages log files in a directory that does not have strict access controls. This allows a low privileged user to manipulate these files, potentially leading to privilege escalation. The service performs file rename/move operations recursively, and if manipulated correctly, this behavior can be abused to perform unauthorized actions.
- **Mitigation:** Users are advised to update their VirtualBox to version 7.0.16 or later, which contains the necessary patches to mitigate this vulnerability.

III. AFFECTED INDUSTRIES

A. IT and Software Development

- **Virtualization Infrastructure:** IT companies and cloud service providers often use VirtualBox for creating and managing virtual environments. Exploitation of this vulnerability could lead to unauthorized access and control over virtual machines, compromising the integrity and confidentiality of hosted services and data.
- **Service Disruption:** A successful attack could disrupt services provided to clients, leading to downtime and potential financial losses.

B. Education and Training

- **Research Data:** VirtualBox is used for research and academic purposes. Unauthorized access could compromise research data and intellectual property.
- **Service Availability:** Disruption of virtualized environments affect online learning platforms and administrative functions.

C. Cybersecurity and Forensics:

- **Data Security:** Cybersecurity and forensics professionals often use virtual machines to analyze malware, conduct penetration testing, and perform forensic investigations in isolated environments. A compromised VirtualBox could lead to unauthorized access to sensitive forensic data and tools, potentially compromising the integrity of investigations.
- **Unauthorized Access:** Attackers gain access to forensic tools and data, manipulate evidence, or disrupt ongoing investigations by escalating privileges.

D. Enterprise and Business:

- **Customer Data:** Enterprises and businesses use VirtualBox for various purposes, including software development, testing, and running legacy applications. A successful exploit could lead to unauthorized access to corporate data, intellectual property, and critical business applications.
- **Operational Impact:** The vulnerability could result in data breaches, loss of sensitive information, and disruption of business operations, leading to financial and reputational damage.

E. Product Demonstrations and Sales:

- **Customer Data:** VirtualBox is often used for product demonstrations and sales presentations to showcase software and solutions in a controlled environment. An attacker exploiting this vulnerability could disrupt demonstrations, access proprietary software, or manipulate the demonstration environment.
- **Brand Impact:** This could lead to loss of customer trust, potential exposure of proprietary software, and negative impacts on sales and marketing efforts.

F. Industrial Automation:

- **Automation Infrastructure:** In industrial automation, VirtualBox may be used to simulate and test automation systems before deployment. A compromised VirtualBox could lead to unauthorized access to industrial control systems, potentially causing disruptions in manufacturing processes.
- **Service Disruption:** This could result in production downtime, safety hazards, and financial losses due to disrupted manufacturing operations.

G. Remote Work and Virtual Desktops:

- **Sensitive Data:** VirtualBox is widely used to provide virtual desktop environments for remote workers. Exploiting this vulnerability could allow attackers to gain control over virtual desktops, access sensitive corporate data, and disrupt remote work operations.
- **Data Leakage:** This could lead to data breaches, loss of productivity, and increased security risks for remote workers and the organizations they work for.

H. Financial Services:

- **Data Security:** Financial institutions use virtualization to isolate sensitive data and applications. An attacker gaining SYSTEM privileges could access, modify, or delete sensitive financial data, leading to severe regulatory and financial repercussions.
- **Compliance Risks:** Breaches could result in non-compliance with financial regulations and standards, attracting penalties and damaging reputation.

I. Healthcare:

- **Patient Data:** Healthcare providers use virtualized environments to manage patient records and other sensitive information. Exploitation of this vulnerability could lead to unauthorized access to patient data, violating privacy laws such as HIPAA.

- **Operational Impact:** System takeovers could disrupt critical healthcare services, affecting patient care and operational efficiency.

J. Government and Defense:

- **National Security:** Government agencies and defense organizations use virtualization for secure and efficient operations. A breach could lead to unauthorized access to classified information, posing national security risks.
- **Operational Disruption:** Compromised systems could disrupt essential government services and defense operations.

IV. ROOT OF CAUSE

The root cause of CVE-2024-21111 in Oracle VM VirtualBox is a local privilege escalation vulnerability that stems from the improper handling of symbolic links and file operations within the VirtualBox environment.

- **Symbolic Link Following:** The vulnerability allows for the exploitation of symbolic link following, where VirtualBox, running with system-level privileges, attempts to move or delete log files in the C:\ProgramData\VirtualBox directory. This directory and its operations are accessible and writable by all users.
- **Improper File Handling:** VirtualBox tries to manage log files by moving them to back them up and deleting the oldest log when more than ten logs exist. This operation is performed without proper validation or security checks to ensure that the files being manipulated are not maliciously linked to other critical system files or directories.
- **Insecure Permissions:** C:\ProgramData\VirtualBox directory inherits permissions that allow all users to create and modify files. This lax permission setting enables low-privileged users to create symbolic links that can redirect file operations intended for log files to any other file or directory, leading to unauthorized actions being performed with elevated privileges.

V. ATTACK FLOW & SCENARIO

CVE-2024-21111 is a local privilege escalation vulnerability in Oracle VM VirtualBox, specifically affecting Windows hosts.

A. Attack flow

- **Initial Access and Environment Setup:** The attacker must have low-level user privileges and logon access to a system where Oracle VM VirtualBox is installed. The versions affected are prior to 7.0.16.
- **Exploitation of Symbolic Link Following:** The core of the vulnerability lies in the exploitation of symbolic link following within the VirtualBox environment. This allows the attacker to perform unauthorized actions such as arbitrary file deletion and movement.
- **Manipulation of Log Files:** VirtualBox attempts to manage log files under the directory C:\ProgramData\VirtualBox. These files are handled by the system with elevated privileges. The system tries to move these log files to back them up, maintaining only the latest 10 logs and attempting to delete the 11th log.

- **Privilege Escalation:** Due to the vulnerability, the attacker can exploit the way VirtualBox handles these log files to escalate their privileges. By manipulating the symbolic links or the log files themselves, the attacker can force the system to execute arbitrary actions with system-level privileges.
- **System Takeover:** Once the attacker has escalated their privileges to the system level, they can execute further malicious activities, leading to a full system takeover.

B. Attack Scenario

1) Initial Setup

- **Environment:** Windows system running a vulnerable version of Oracle VM VirtualBox (prior to 7.0.16).
- **Permissions:** The attacker has low-level user access with the ability to log on to the system.

2) Exploitation Steps

- **Identify Target Directory:** The attacker identifies the C:\ProgramData\VirtualBox directory, which is used by VirtualBox to store log files. This directory is writable by all users, which is a key factor in the exploitation.
- **Create Symbolic Links:** The attacker creates symbolic links in the C:\ProgramData\VirtualBox directory to redirect file operations (such as move or delete) to critical system files or directories.
- **Trigger File Operations:**
 - **Move Operation:** When VirtualBox attempts to move a log file, it instead moves the targeted file, potentially causing unauthorized file movements.
 - **Delete Operation:** When VirtualBox attempts to delete an old log file, it instead deletes the targeted system file.
- **Privilege Escalation:** By manipulating these file operations, the attacker performs actions that are normally restricted to higher-privileged accounts. This leads to the escalation of privileges to the highest level of privilege on Windows systems.

3) Post-Exploitation

- **System Takeover:** With SYSTEM privileges attacker:
 - Execute elevated arbitrary commands.
 - Access and modify any file on the system.
 - Install malicious software or backdoors.
 - Create new accounts with administrative privileges.
- **Persistence and Lateral Movement:** The attacker can establish persistence mechanisms to maintain access to the compromised system and potentially move laterally within the network to compromise additional systems.

VI. POC

The GitHub repository for CVE-2024-21111, hosted by manskles, details a Local Privilege Escalation (LPE) vulnerability in Oracle VirtualBox versions

- **Affected Component:** The vulnerability affects the way VirtualBox handles log files. VirtualBox, running as NT

AUTHORITY\SYSTEM, attempts to move log files within C:\ProgramData\VirtualBox to back them up by an ordinal system, maintaining a maximum of 10 logs. When the number of logs exceeds this limit, VirtualBox tries to delete the 11th log.

- **Exploitation Mechanism:** The exploitation of this vulnerability is facilitated by the fact that the C:\ProgramData\VirtualBox directory is writable by all users. This allows an attacker to exploit the process of moving and deleting log files to escalate privileges. The vulnerability exposes two bugs related to this process that can lead to privilege escalation.
- **Privilege Escalation Path:** By exploiting the symbolic link following vulnerability, an attacker can manipulate the file operations performed by VirtualBox (as NT AUTHORITY\SYSTEM) to achieve arbitrary file deletion or movement. This can lead to unauthorized actions being performed with system-level privileges

The GitHub repository for CVE-2024-21111 provides proof of concept (PoC) scripts that demonstrate the local privilege escalation vulnerability in VM VirtualBox are in the directories VirtualBoxLPE_move and VirtualBoxLPE_del.

A. Input Data for Scripts

- The path to directory (C:\ProgramData\VirtualBox), which is where VirtualBox manages log files.
- Specific parameters or configurations that mimic the operations performed by VirtualBox, such as moving or deleting log files.

1) VirtualBoxLPE_move:

This script requires input specifying which log files to move and the new location or manner in which these files should be moved. The input could also include the creation of symbolic links that redirect these operations to unintended targets.

2) VirtualBoxLPE_del:

Like the move script, this deletion script relates on input specifying which log files to delete. The script might also involve the creation of symbolic links that cause the deletion operation to affect unintended files or directories.

B. Outcomes After Running the Scripts

1) VirtualBoxLPE_move:

After running this script, the outcome is that the log files are moved in a way that exploits the symbolic link following vulnerability. This leads to unauthorized file movements, potentially allowing an attacker to relocate system files or other sensitive files to locations with less secure permissions.

2) VirtualBoxLPE_del:

The outcome of running this deletion script is the deletion of files or directories that were not originally intended to be deleted. By exploiting the symbolic link following, an attacker could redirect the deletion process to remove critical system files or other protected data, leading to system instability or further security compromises.