KVM Switcher Vulnerability

Overview

The vulnerability, identified as CVE-2024-50386, affects Apache CloudStack versions 4. This security issue stems from missing validation checks for KVM-compatible templates during the template registration process. KVM (Keyboard, Video, and Mouse) switches have become an essential component in many industries, including finance, government, and healthcare, where multiple computers need to be accessed and managed from a single workstation. These devices allow users to switch between different computers. The Apache CloudStack project has announced the release of critical security updates to address severe vulnerabilities in its KVM-based infrastructure. Administrators often use them to remotely access machines on networks. The. growing more common and complex with each passing day. Massive high-profile cybersecurity breaches such as the Solar Winds supply chain attack in 2020 have brought organizations worldwide a greate sense of urgency in protecting against cyber threats. The nine vulnerabilities, discovered by Eclypsium, span four different products from GL-iNet. Last September, the police arrested criminals who conspired to steal millions of dollars from Barclays Bank and Santander Bank.

Article Content

from Cyber Threats with the Latest KVM Technology

Secure KVM for State and Local Government Many federal government agencies mandate the use of NIAP certified secure keyboard-video-mouse (KVM) switches at operator stations that need access

Meeting Cybersecurity Threats With Secure KVM Switches

Together, these features and capabilities enable a secure KVM switch to address the requirements of the most demanding applications, including deployment in government and military environments.

Can a KVM Switch be Hacked? Understanding the Risks and Mitigations

However, like any other network device, KVM switches are not immune to cybersecurity threats. The question on everyone''s mind is, can a KVM switch be hacked? In this article, we will

CVE-2025-3710: Critical Buffer Overflow Vulnerability in LCD KVM

Overview The Common Vulnerabilities and Exposures (CVE) system has recently identified a critical vulnerability, CVE-2025-3710, within the LCD KVM over IP Switch CL5708IM. This

9 Critical IP KVM Flaws Enable Unauthenticated Root

Researchers uncovered 9 vulnerabilities across 4 IP KVM devices enabling unauthenticated root access and code execution.

A flaw was found in KVM AMD Secure Encrypted...

Description A flaw was found in KVM AMD Secure Encrypted Virtualization (SEV) in the Linux kernel. A KVM guest using SEV-ES or SEV-SNP with multiple vCPUs can trigger a double

Are KVM Switches a Security Risk? Understanding the Vulnerabilities

One of the most significant security risks associated with KVM switches is data leakage and eavesdropping. Since the switch has access to all connected computers, a compromised KVM

CVE-2025-3711: LCD KVM over IP Switch Vulnerability

CVE-2025-3711 identifies a critical security flaw in the LCD KVM over IP Switch model CL5708IM. This vulnerability arises from a stack-based buffer overflow, posing significant risks to

Researchers disclose vulnerabilities in IP KVMs from four manufacturers

On Tuesday, researchers from security firm Eclypsium disclosed a total of nine vulnerabilities in IP KVMs from four manufacturers. The most severe flaws allow unauthenticated

Cybersecurity Concerns?

Administrator Configuration and Event Log Functions — User friendly interface for authorized administrator to audit critical KVM operation logs and perform KVM switch configuration.

Researchers disclose vulnerabilities in IP KVMs from four manufacturers

No exotic zero-days here On Tuesday, researchers from security firm Eclypsium disclosed a total of nine vulnerabilities in IP KVMs from four manufacturers.

CVE-2025-3711: Critical Stack-based Buffer Overflow Vulnerability in ...

Overview CVE-2025-3711 is a severe cybersecurity vulnerability that affects the LCD KVM over IP Switch CL5708IM. This vulnerability, a stack-based buffer overflow, exposes the system

FBI investigates KVM threats, visits tech r

Despite the relative newness of KVM devices, runZero has already found hundreds of them publicly exposed on the IoT search engine Shodan. The

The Hidden Risks of KVM Devices in Cybersecurity

The article discusses the potential cybersecurity risks associated with KVM (Keyboard, Video, Mouse) devices, particularly those that are not professionally vetted. It highlights a specific

$30 IP-KVM Vulnerabilities Expose Enterprises to BIOS-Level Attacks

A new wave of security research has uncovered critical flaws in low-cost IP-KVM (Keyboard, Video, Mouse) devices, raising serious concerns for enterprise environments.

10 ways to address KVM switch vulnerabilities -

The internal and external components of the switch may be vulnerable to tampering. In light of these vulnerabilities, best practices have emerged that allow government security professionals to address

CVE-2025-3714 : The LCD KVM over IP Switch CL5708IM has a

The LCD KVM over IP Switch CL5708IM has a Stack-based Buffer Overflow vulnerability in firmware versions prior to v2.2.215, allowing unauthenticated remote attackers to exploit this

Can a KVM Switch be Hacked? Understanding the Risks and

A KVM switch is a hardware device that allows users to control multiple computers from a single keyboard, mouse, and monitor. While KVM switches offer convenience and flexibility, they

Understanding CVE-2024-39483: A Closer Look at KVM Virtualization ...

Understanding CVE-2024-39483: A Closer Look at KVM Virtualization Vulnerability Welcome to another important update on Linux security. Today, we delve into a recently disclosed vulnerability tracked as

Your KVM is the Weak Link: How $30 Devices Can

Eclypsium researchers discovered 9 vulnerabilities across 4 low-cost IP-KVM vendors, exposing fundamental security failures that give attackers the

Your KVM is the Weak Link: How $30 Devices Can

Researchers at grumpygoose.io published a detailed analysis of the TinyPilot KVM, including a companion post on unemployfuscation techniques

Strengths And Weaknesses Of Using KVM Switches Over TCP/IP

It will discuss the situation before the advent of KVM using TCP/IP, and the benefits of using this new technology, along with the inherent risks involved. Five different models of switches will be briefly

from Cyber Threats with the Latest KVM Technology

Secure keyboard-video-mouse (KVM) switches allow access to multiple computing systems at diferent security classifications, from a single desktop. This segregates secure and non-secure computing

10 ways to address KVM switch vulnerabilities

The internal and external components of the switch may be vulnerable to tampering. Best practices for boosting security In light of these vulnerabilities, best practices are emerging that allow

Apache CloudStack Released Fix for Critical KVM

Exploiting this vulnerability could enable attackers to deploy malicious instances, potentially gaining unauthorized access to host filesystems

Contact Us

For more information, pricing, or custom solutions, please contact us:

Website: https://saastisfy.fr
Email: sales@saastisfy.fr
Phone: +33 6 52 81 47 39
Address: 75 Rue de Rivoli, 75001 Paris, France

This document is for informational purposes only. Specifications subject to change without notice.