KVM switcher has security vulnerabilities



Overview

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 hackers to gain root access or run malicious code on them. Researchers are warning about the risks posed by a low-cost device that can give insiders and hackers unusually broad powers in compromising 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. 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. These devices, often priced between $30 and $100, are increasingly used for remote system management but are now being weaponized. While KVM switches offer many benefits, they also introduce potential security risks, including: One of the most significant security risks associated with KVM switches is data leakage and eavesdropping.

© 2026 AK OPTICAL SYSTEMS - All rights reserved

Article Content

Researchers disclose vulnerabilities in IP KVMs from

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

9 Critical IP KVM Flaws Enable Unauthenticated Root

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

$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.

Meeting Cybersecurity Threats With Secure KVM Switches

Built with true data-path isolation between systems and networks to ensure no data is leaked between secure ports and the outside world, secure KVM devices are the hidden champions in providing an

Are KVM Switches a Security Risk? Understanding the Vulnerabilities

However, as with any technology, KVM switches are not immune to security risks. In this article, we will delve into the potential security vulnerabilities associated with KVM switches and

IP KVM Vulnerabilities Exposed: Critical Security Flaws Threatening ...

Researchers have uncovered alarming IP KVM vulnerabilities embedded in the firmware of four major manufacturers, putting data centers, government agencies, and critical infrastructure at

Apache CloudStack Released Fix for Critical KVM

The Apache CloudStack project has announced the release of critical security updates to address severe vulnerabilities in its KVM-based infrastructure.

Critical IP KVM Vulnerabilities Expose Servers To Pre-Boot Remote

Once an IP KVM is compromised, an attacker can control the server''s console, alter firmware settings, boot malicious images, and bypass host-based security controls such as EDR,

Black Box KVM

© 2026 AK OPTICAL SYSTEMS - All rights reserved

Black Box KVM Firmware version 3.4.31307 on models ACR1000A-R-R2, ACR1000A-T-R2, ACR1002A-T, ACR1002A-R, and ACR1020A-T is vulnerable to path traversal, which may allow an attacker to

IP KVM Devices Hit by Nine Critical Security Flaws

Security researchers at Eclypsium published findings on March 18, 2026, revealing nine critical vulnerabilities affecting low-cost IP KVM devices

What are Secure KVM Switches?

Secure KVM switches are designed from the ground up as dedicated switching devices with every element conceived to prevent unauthorized access and

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

Meeting Cybersecurity Threats With Secure KVM Switches

This white paper explores the critical role of secure KVM switches in mitigating cyber threats, emphasizing the importance of the NIAP Protection Profile V4.0. It highlights the switch''s role in

Can a KVM switch be vulnerable through a VGA port?

I have one KVM switch that has a VGA port to connect monitor. I want to know how to test that the KVM switch has no vulnerabilities by this port (using DDC)?

KVM switches security : r/techsupport

If by leakage you mean conveying information such as mouse movements, keystrokes etc. from the currently active/selected machine to the other machine, then yes it''s technically possible if the KVM

Is it possible to transfer malware/viruses through a KVM Switch, from ...

So essentially is it possible to transfer malware through a KVM switch, and how likely is something like this to occur? EDIT: Just found this Can a KVM switch be vulnerable through a VGA

IP KVM Vulnerabilities Exposed: Critical Security Flaws Threatening ...

IP KVM vulnerabilities have emerged as one of the most alarming cybersecurity threats facing enterprise and data center environments today. Researchers have uncovered a sweeping set

CVE-2025-3714: Stack-based Buffer Overflow Vulnerability in LCD KVM ...

© 2026 AK OPTICAL SYSTEMS - All rights reserved

Overview The cybersecurity world is witnessing a new vulnerability in the LCD KVM over IP Switch CL5708IM that has a Stack-based Buffer Overflow vulnerability. This vulnerability,

Related Video Reference

This video was associated with the source search result. Verify technical details against current product documentation and project requirements.

Contact Us

Continue your research online:

Website: https://aboutkitchens.biz
Technical inquiry: https://aboutkitchens.biz/project-desk.html
North American project location: Research Triangle Park, North Carolina, United States

This document is for preliminary research. Verify specifications against current standards, product documentation and project requirements.

© 2026 AK OPTICAL SYSTEMS - All rights reserved