LEGION cyberworks

Security Risk Brief: Lenovo Devices

Overview

Lenovo's low-cost computers dominate U.S. SLED and private sector markets. But these savings come with hidden costs: a long track record of cyber vulnerabilities, firmware-level flaws, and troubling ties to potential surveillance risks.

July 16, 2025

Key Incidents

1 Espionage Allegations (2008)

U.S. military investigators allegedly found hidden chips logging keystrokes. Lenovo denied involvement.

2 Superfish Adware (2014-2015)

Injected ads via a universal root certificate, enabling HTTPS traffic interception. Resulted in $8.3M class-action and $3.5M FTC fine.

3 Lenovo Service Engine (2014-2015)

BIOS-level installer reinstalled apps on every reboot, violating Microsoft security guidance.

4 Lenovo Accelerator (2016)

Pre-installed software with HTTPS proxy vulnerabilities, exposing users to man-in-the-middle (MITM) attacks.

5 UEFI/BIOS Vulnerabilities (2021-2022)

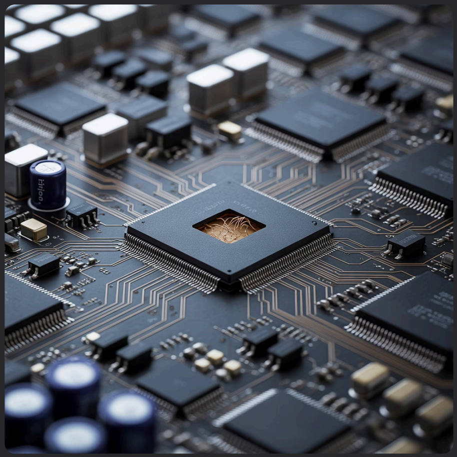
CVEs exposed Secure Boot to disablement and permanent malware implantation. Older models remain unpatched.

Strategic Risk

Lenovo's aggressive pricing secures mass adoption across government, education, and enterprise markets, particularly in budget-constrained sectors. However, this price-driven strategy carries hidden costs that introduce serious cybersecurity and geopolitical concerns.

Complex auditability and patching:

Firmware-level vulnerabilities and pre-installed software components make Lenovo devices harder to audit, update, or reimage cleanly—posing persistent risks to endpoint security.



Supply chain integrity concerns:

Repeated incidents involving low-level firmware and UEFI tampering demonstrate how devices can be compromised before reaching end users, potentially giving attackers long-term access.

Geopolitical entanglements:

Lenovo's partial state ownership and historic ties to entities linked with the Chinese Communist Party raise serious questions about data sovereignty, particularly for SLED organizations handling sensitive public records or infrastructure controls.

In combination, these factors shift the Lenovo conversation from a cost-saving discussion to a risk mitigation imperative.

Recommendations

Stop Procurement

Cease procurement of Lenovo hardware for sensitive operations

Audit Devices

Audit current devices for firmware integrity and known exploits

Isolate Systems

Isolate or retire Lenovo systems in mission-critical environments

New Policies

Introduce procurement policies that prioritize security and supply chain transparency

Citations

CISA: Lenovo Superfish HTTPS Spoofing - **https://www.cisa.gov/news-events/alerts/2015/02/20/lenovo-superfish-adware-vulnerable-https-spoofing**

Wired: Lenovo Superfish Scandal - **https://www.wired.com/story/lenovo-superfish**

Heimdal Security: UEFI Firmware Vulnerabilities - **https://heimdalsecurity.com/blog/millions-of-laptops-impacted-by-lenovo-uefi-firmware-vulnerabilities**

Wikipedia: Lenovo Overview - **https://en.wikipedia.org/wiki/Lenovo**

Tom's Hardware: Settlement Details - **https://www.tomshardware.com/news/lenovo-settlement-superfish-scandal-progress%2C38657.html**

Supplemental Brief: Lenovo Origins and State Influence

Background Lenovo was founded in 1984 under the name Legend by a team of engineers from the Chinese Academy of Sciences (CAS), a state-run research institute. The company received initial funding from CAS and grew rapidly, rebranding as "Lenovo" in 2003 to expand globally.

Ownership and Ties to the CCP Lenovo is partially owned by **Legend Holdings**, which itself is approximately 29% owned by the Chinese Academy of Sciences. CAS is a major entity within the Chinese state apparatus and plays a role in advancing strategic technologies.

As of recent public filings:

- Legend Holdings owns roughly **31–36%** of Lenovo
- Other shareholders include Chinese government-linked investors
- Lenovo maintains dual headquarters in **Beijing and North Carolina**, but remains a Hong Kong-listed firm

Why This Matters These ties raise important questions for SLED and enterprise cybersecurity planners:

- **Supply chain exposure**: Foundational ownership links to state entities raise the risk of influence over hardware and firmware-level operations.
- **Data sovereignty**: Devices built under potential government-influenced directives could compromise the confidentiality of sensitive or regulated information.
- **Procurement risk**: Increasing attention from U.S. lawmakers and cybersecurity agencies toward Chinese-owned tech suppliers could lead to future policy restrictions or bans.

Foundational State Ties

Lenovo's direct origin as a CAS spin-off means its governance structure is inherently linked to a state research institute, creating a deep-rooted channel for potential state influence.

Strategic Dual-HQ Presence

Despite dual headquarters in Beijing and North Carolina, the company remains listed in Hong Kong with strong institutional ownership rooted in China, complicating accountability.

Perception & Policy Risk

U.S. lawmakers and cybersecurity officials have explicitly flagged Lenovo's ties to CCP and PLA-linked entities, leading to increasing scrutiny and potential procurement restrictions.

Lenovo Back Story

Aspect	Details
Founded	1984 by Liu Chuanzhi & colleagues, as Legend with CAS support
Public Offering	Hong Kong IPO in 1994
Rebrand & Expansion	Became Lenovo in 2003; acquired IBM PC in 2005
Ownership	~31–36% owned by Legend Holdings (CAS-linked)
Governance	CAS retains influence via state investment; Lenovo claims operational independence
Security Concern	Institutional ties to CAS/CCP raise potential for influence and government direction

Source Highlights

- https://en.wikipedia.org/wiki/Lenovo
- https://en.wikipedia.org/wiki/Legend_Holdings
- https://www.tomshardware.com/news/lenovo-denies-chinese-government-ties-as-us-lawmakers-ask-questions
- https://selectcommitteeontheccp.house.gov/media/press-releases/gallagher-urges-us-navy-exchange-remove-ccp-linked-computers-stores

About Legion Cyberworks

Partner With a Proven Cybersecurity Team

If your organization is reassessing its technology stack or looking for a proactive cybersecurity partner, Legion Cyberworks is here to help. With a proven track record in protecting clients from complex cyber threats, we offer the insight and tools to help you stay secure.

Our Exemplary Services

- 24×7 SOC & MXDR Services
- SIEM, EDR, ITDR
- Offensive Security Services (Red Teaming, Pentesting, AI Autonomous)
- Vulnerability Scanning
- Cloud Security
- Web and API Defense
- Darkweb Monitoring & Account Takeover Prevention

Contact Legion Cyberworks:
📞 919-769-2916
🌐 **legioncyber.com**
✉️ sales@legioncyber.com

LEGION
cyberworks