Phosphorus, A Dragos Company
DATA SHEET

Phosphorus xIoT Firmware Management

Eliminate exploitable weaknesses. Keep firmware current, safely.

The Challenge

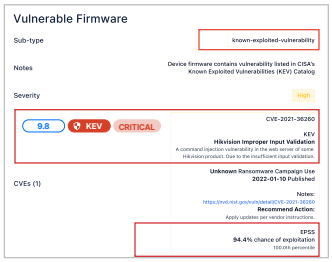
Firmware is the hidden operating system for **x**IoT devices and is often their weakest link. Printers, IP cameras, PDUs, HVAC controllers, access control systems, and countless other devices frequently run outdated or vulnerable firmware for years. The risks include:

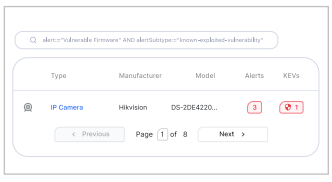
- Exploitable vulnerabilities with known CVEs leave them exposed to ransomware and targeted attacks.
- Hidden, banned Chinese-sourced firmware with embedded malicious backdoors.
- Limited visibility into which devices are running insecure or end-of-life firmware.
- Firmware updates that unintentionally introduce new instabilities or risks.

Attackers exploit these weaknesses to gain footholds, persist undetected, and disrupt mission-critical operations. Traditional IT vulnerability management tools are unable to handle the diversity, sensitivity, and operational requirements of **x**IoT environments to address this risk. Furthermore, most organizations lack operational workflows to keep thousands of devices up to date at scale.

The Phosphorus Advantage

Phosphorus, now part of the Dragos portfolio, delivers the industry's first and only **x**IoT Security and Management Platform that automates firmware vulnerability management safely, comprehensively, and at scale.



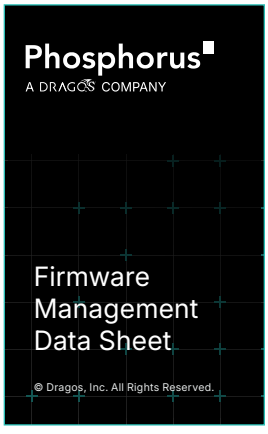


1. **Automated Firmware Discovery & Risk Context**
   Identify firmware versions across all device estates, enriched with CVE, KEV, and EPSS data to prioritize and remediate exploitable vulnerabilities.
2. **Safe Upgrades and Downgrades**
   Upgrade to secure vendor firmware or downgrade to stable versions to maintain security and stability against known exploits.
3. **Phosphorus Firmware Content Delivery Network**
   Access a secure global repository of vendor-supplied firmware binaries, enabling faster updates and the remediation of end-of-life devices.
4. **Hidden Risk Discovery & Firmware Validation**
   Detect and remove devices with banned or backdoored Chinese firmware, validate integrity for NDAA compliance, and automatically isolate risky devices.
5. **Operationalizing Firmware Maintenance at Scale**
   Automate recurring firmware maintenance with scheduled jobs, enforcing global policies and applying upgrades or downgrades via granular rules.
6. **Continuous Monitoring**
   Detect drift when firmware becomes outdated or misaligned with policy, and remediate before attackers exploit it.

AT A GLANCE

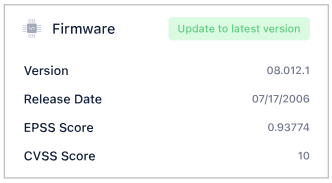
Key Benefits

- Automatic discovery of device firmware versions
- Risk context from CVE, KEV, and EPSS
- Upgrade or downgrade safely at scale
- Policy-driven automation with recurring jobs
- Firmware CDN for post-vendor support remediation
- Maintain firmware currency without disruption



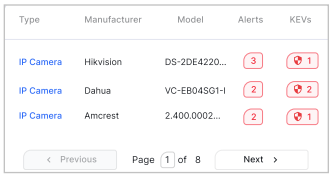
Customer Outcomes

With Phosphorus, enterprises and organizations across critical infrastructure achieve:



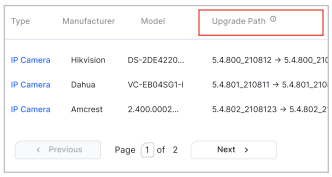
Immediate Visibility into Firmware Versions and Risks

Instantly identify device firmware versions and their associated security exposures.



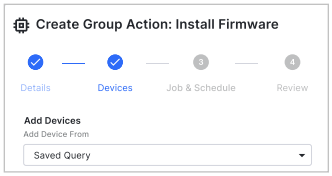
Risk-Prioritized Remediation Informed by CVE, KEV, and EPSS

Address vulnerabilities based on real-time threat intelligence and exploit likelihood.



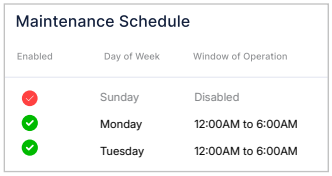
Safe Upgrades and Downgrades Tailored to Device Criticality

Ensure firmware changes align with each device's operational importance and safety requirements.



Ongoing Firmware Currency, Maintained by Automated Recurring Jobs

Keep all devices up to date through continuous, automated firmware management.



Reduced Manual Operational Overhead Through Automation

Streamline security maintenance by eliminating repetitive manual tasks.

For CISOs and CIOs

Phosphorus delivers strategic resilience by unifying fragmented device security processes into a single autonomous platform. It empowers leadership to ensure enterprise-wide compliance, reduce attack surface risk, and extend zero-trust principles to their entire **x**IoT environments.

Why Phosphorus

We secure and manage connected devices at machine scale; safely, automatically, continuously, with human oversight, not limitations.

DISCOVER AND ASSESS

- ✓ Asset Discovery
- ✓ Vulnerability Assessment
- ✓ Prohibited Device Detection and Response

HARDEN & REMEDIATE

- ✓ Password Management
- ✓ **Firmware Management**
- ✓ Certificate Management
- ✓ Configuration Management

MONITOR & MANAGE

- ✓ Device State Monitoring
- ✓ Device Log Retrieval
- ✓ Device Backup

FAST VALUE REALIZATION

Deploys quickly with no agents, hardware, SPAN ports, or packet brokers.

LEVERAGE EXISTING INVESTMENTS

Integrates with SIEM, SOAR, PAM, and ITSM systems for complete downstream visibility.