KALEN

VALIDATING TRUST ACROSS THE GRID

POWERED BY GRID FRAMEWORK

Issue 04

Monthly Member Publication

KALEN INTELLIGENCE BRIEF

ISSUE No. 4 · SEPTEMBER 2026

Validating Trust Across the Grid. Informing What Comes Next.

CYBERSECURITY | CRITICAL INFRASTRUCTURE | ARTIFICIAL INTELLIGENCE | IDENTITY SECURITY | SUPPLY CHAIN | FEDERAL POLICY

utc.org/KALEN
Utilities Technology Council

Utilities Technology Council

A Message from UTC

Office of the Vice President, Cybersecurity & Advocacy



Cordell Briggs

Vice President,
Cybersecurity & Advocacy

Utilities Technology Council

Most of the incidents covered in past issues of this brief targeted a single utility, plant, or system at a time. This month's developments point to something different: attackers, and increasingly AI acting on their behalf, targeting the shared infrastructure that connects hundreds of organizations at once.

A single compromised device at a metering technology vendor exposed credentials for 167 utility customers. Actively exploited flaws in Cisco's firewall management console and other administrative platforms put entire fleets of managed devices at risk because of a single point of failure.

A threat actor also, for the first time at this scale, demonstrated that AI agents can independently develop exploits and compromise hundreds of organizations in hours, not weeks.

The KALEN™ Intelligence Brief helps UTC members understand developments like these before they become operational, procurement, compliance, or business challenges.

This month, we examine DOE's new request for public input on implementing the bulk-power system executive order; NERC's continued work on cloud services standards; a landmark AI-driven exploitation campaign; a new federally backed AI defense tool for the grid; actively exploited vulnerabilities in widely used network and remote-management platforms; and new research on credential exposure across the water sector.



Regulatory & Standards Watch

DOE Opens Comment Period on Bulk-Power System Executive Order

On September 9, 2026, DOE's Office of Cybersecurity, Energy Security, and Emergency Response published a Request for Information seeking public input on implementing Executive Order 14421, the national emergency declaration regarding foreign-sourced bulk-power system equipment, as covered in last month's issue.

The RFI is organized into eight topic areas and poses more than 50 questions covering the scope of covered equipment, Covered Foreign Entity determinations, software and firmware risk, existing equipment and mitigation, and licensing and prequalification. DOE held a public webinar on September 16, 2026. Written responses are due by October 9, 2026, via the federal eRulemaking portal under docket DOE-HQ-2026-1123 or by email to BulkPowerEO@doe.gov.



Why It Matters

- Utilities and suppliers with a stake in how DOE defines Covered Foreign Entity, qualifying equipment, or prequalified vendor status should submit comments by October 9. This RFI is the clearest opportunity yet to shape the rules before they're finalized.
- DOE's final implementing rules are still expected by late December 2026, with recommended federal procurement changes to follow in February 2027.
- Entities that haven't yet inventoried foreign-sourced bulk-power system equipment should treat this RFI period as a prompt to begin now, rather than waiting for the final rule.

NERC's Cloud Services Standards Move Into Revision

NERC's Project 2023-09 drafting team is now reviewing the industry comments submitted during the informal comment period, which closed on August 21. Per NERC's standards development plan, drafting on the five proposed CIP 100-series standards (CIP-002-9, CIP-102-1, CIP-103-1, CIP-105-1, and CIP-113-1) is expected to continue through December 2026, with a formal ballot still to come.

Industry feedback during the comment period raised a real scoping question. Some drafting team members have acknowledged that entities that don't plan to use cloud services may still be affected by the new standards in ways that remain unresolved. That question remains open as the drafting team reviews the comments received.

Why It Matters

- Utilities and suppliers should continue monitoring Project 2023-09 rather than treating the closed comment period as the end of the process. A formal ballot has not yet been scheduled.
- The scoping question raised during the comment period warrants close tracking, since it could affect entities that assumed the standards wouldn't apply to them.

Critical Infrastructure Cyber Alert

Actively Exploited Flaws in Network Management Platforms Put Device Fleets at Risk

Active, ongoing exploitation across multiple vendors. See the Recommended Actions below.

Since early September, security researchers and vendors have confirmed active exploitation of critical vulnerabilities in the platforms organizations use to manage and administer their network and security infrastructure. On September 9, Cisco confirmed that two vulnerabilities in its Secure Firewall Management Center (FMC), including CVE-2026-20079, a maximum-severity flaw that allows an unauthenticated attacker to execute commands as root, are being actively exploited by at least three threat groups. FMC is the console that pushes policy and configuration to every firewall it manages, so compromising it can compromise the entire fleet at once.

The same week, F5 disclosed CVE-2026-94127, a critical, actively exploited remote code execution flaw in BIG-IP's access management module. CISA added it to its Known Exploited Vulnerabilities catalog. Similar high-risk disclosures affected VMware, SonicWall, and at least one widely used remote monitoring and management platform this month, continuing a pattern of attackers targeting the administrative layer that manages infrastructure rather than individual endpoints.



WHY THIS MATTERS

- Utilities and suppliers running Cisco Secure Firewall Management Center should patch immediately. Cisco has confirmed there is no workaround for the most severe flaw.
- Organizations using F5 BIG-IP, VMware, SonicWall, or third-party remote management platforms should now verify current patch levels against each vendor's advisories. Several of these flaws are already in CISA's Known Exploited Vulnerabilities catalog.
- A single compromised management platform can expose every device it manages, so these platforms deserve the same urgency as internet-facing OT devices.

Operational Considerations

- ✓ Patch Cisco Secure Firewall Management Center and check for signs of prior compromise, as exploitation was underway before the flaw was confirmed.
- ✓ Check versions of F5 BIG-IP, VMware, SonicWall, and the remote management platform against each vendor's September 2026 advisories and CISA's KEV catalog.
- ✓ Review administrative and remote access to management consoles and restrict internet exposure wherever possible.
- ✓ Prioritize patching for management-plane platforms, firewall managers, identity systems, and remote monitoring tools, on par with customer-facing systems, not as an afterthought.

Artificial Intelligence Watch

AI Agents Independently Compromised 395 Organizations in Days

In late August, a threat actor built and deployed a swarm of autonomous AI agents to exploit two vulnerabilities in PaperCut NG/MF print management software, CVE-2026-81578 and CVE-2026-82078, with limited apparent human direction after the initial setup.

Research published September 9 by GreyNoise and Blackpoint Cyber found that the campaign compromised at least 440 servers across 395 organizations in 48 countries. In one case, the agents took a U.S. high school from initial access to full domain administrator control in seven minutes, and at peak speed compromised 11 organizations in 26 seconds.

In a detail researchers flagged as particularly notable, the AI agents deviated from the attacker's instructions and compromised organizations in countries the attacker had explicitly excluded. GreyNoise described it simply as agents gone wild.

PaperCut is primarily an IT system rather than an OT platform, and education was the hardest-hit sector. The campaign is one of the clearest public demonstrations yet that AI can independently perform exploit development, scanning, and post-exploitation work at a speed no human security team can match.

Why It Matters

- Utilities and suppliers should recognize that the gap between a vulnerability disclosure and mass exploitation is shrinking to hours, not weeks, when AI tooling is involved.
- Any internet-facing administrative system, not just OT devices, is now a plausible target for this type of automated, AI-driven campaign.
- AI agents deviating from their operators' instructions is a reminder that AI-driven attacks may not behave predictably, complicating both defense and attribution.



DOE and Sandia National Lab Deploy AI to Defend the Grid

The same month AI-driven attacks made headlines, DOE's CESER and Sandia National Laboratories announced Communications and Cybersecurity for the Energy Edge (C2E2), a generative AI tool that helps grid security operators detect and pinpoint the source of cyberattacks.

C2E2 automates power grid data engineering that previously took utility operators up to two months, cutting that work down to a few hours. It is reported to detect threats with roughly 95 percent accuracy.

C2E2 is part of CESER's Artificial Intelligence For Operationally Resilient Technologies and Systems (AI-FORTS) program, the same program behind the Stormbreaker testbed covered in a previous issue. Specifically, it is part of the program's "Secure With AI" pillar, which focuses on applying AI to threat detection, OT and ICS visibility, and incident response.

Sandia's next phase of research will focus on understanding and preventing AI hallucinations, since a hallucination in this context could mean missing a real attack or flagging one that isn't there.

Why It Matters

- Utilities evaluating AI-enabled security tools now have a federally backed reference point for defensive AI in grid environments, developed specifically for this sector rather than adapted from commercial IT tools.
- The hallucination risk that DOE and Sandia are studying applies broadly. Utilities piloting any AI-based detection tool should ask vendors how false positives and false negatives are measured and managed.
- This is the clearest sign yet that AI in the energy sector isn't only a threat to defend against. It's also becoming a tool that utilities are expected to adopt.



Supply Chain & Identity Watch

One Vendor, 167 Utilities: New Research Reveals Widespread Credential Exposure Across the Water Sector

A new study published this month by identity risk firm SpyCloud found that nearly 18 percent of U.S. water and wastewater organizations, 1,787 out of roughly 10,000 analyzed, have active credential exposure due to infostealer malware.

At least 250 of those organizations have credentials that could provide access to operational networks and remote access systems connected to physical control equipment.

One finding stood out. A single malware-infected device at an unnamed metering technology vendor exposed credentials tied to approximately 167 utility customers, illustrating how a single compromised supplier can cascade into exposure for dozens of otherwise unrelated organizations.

Separately, SpyCloud noted that the ongoing Iran-linked attacks on water utilities covered in last month's issue did not rely on stolen credentials. Instead, those attacks exploited default passwords on physical controllers, a distinct vector from the credential exposure described here.

Why It Matters

- Utilities should check whether their credentials or those of key vendors appear in known infostealer datasets and rotate any exposed passwords and session tokens.
- Suppliers, especially those providing metering, monitoring, and other multi-tenant technology, should assume that a single infected device can expose every customer they serve and audit endpoint security accordingly.
- Stolen session tokens can bypass multi-factor authentication, so MFA alone is not sufficient protection against this type of exposure.



KALEN™ Perspective

What This Means for Utilities and Suppliers

This month's developments share a pattern that's easy to miss when viewed individually but consequential when taken together.

Attackers are no longer targeting one at a time. They're targeting the trust layer, shared vendors, credentials, and management systems that connect hundreds of targets at once, and increasingly, AI is doing the targeting.

A single infected device at a single metering vendor exposed credentials for 167 utilities. A single flaw in a firewall management console put every device it administered at risk. In the PaperCut campaign, a single threat actor used AI agents to compromise 395 organizations in a matter of days. In each case, the target wasn't a single utility. It was the shared connective tissue, a vendor, a management console, or a credential store, that many organizations depend on at once.

Meanwhile, the federal response continues to build out the infrastructure this brief has tracked for months. DOE's RFI on the bulk-power system executive order and NERC's ongoing work on cloud services standards are, in their own ways, attempts to formalize how responsibility is shared and verified across exactly these kinds of interconnected relationships.

The scale of the gap is easy to underestimate. A 2026 industry benchmark of OT cybersecurity leaders found that 91 percent of energy and utilities respondents had experienced a significant OT cybersecurity incident in the past 12 months, yet only 21 percent had a complete inventory of their OT assets. Most organizations in this sector are already under pressure and still lack full visibility into what they're defending.

Taken together, these developments raise sharper questions than they did just a month ago:

- Does this organization know which vendors, if compromised, could expose it and dozens of others?
- Are administrative and management-plane systems patched and monitored with the same urgency as customer-facing ones?
- Can this organization independently verify a vendor's security practices rather than relying on the vendor's own word?

For utilities, this means extending scrutiny beyond your own perimeter to the vendors and shared platforms your organization relies on, and verifying, rather than assuming, that those vendors take security as seriously as you do.

For suppliers, especially those serving many utility customers over shared infrastructure, this means a single security failure no longer affects just one customer. It affects every customer you serve, and increasingly, your customers know it.

KALEN™ was built for exactly this kind of interconnected risk. It gives utilities a way to identify suppliers with independently validated cybersecurity credentials, rather than relying on a vendor's own word, and gives suppliers a credible way to demonstrate their maturity before a shared vendor relationship becomes a shared point of failure.

KALEN™ Takeaways

For Utilities

- ✓ Check for credential exposure affecting your organization or key vendors, and rotate any exposed credentials.
- ✓ Patch Cisco Secure Firewall Management Center, F5 BIG-IP, VMware, and RMM platforms immediately to address September's actively exploited vulnerabilities.
- ✓ Submit comments on DOE's bulk-power system RFI before October 9 if your organization has a stake in how equipment or vendor scope is defined.
- ✓ Ask key suppliers, especially shared-infrastructure vendors such as metering platforms, how they'd detect and contain a credential-stealing infection in their own systems.
- ✓ If your organization lacks a complete OT asset inventory, treat it as a foundational gap to close before evaluating any new security tool, AI-enabled or otherwise.

For Suppliers

- ✓ Audit endpoint security across your infrastructure. A single infected device can expose every customer tenant you serve.
- ✓ Patch management plane and administrative platforms with the same urgency as customer-facing systems.
- ✓ Prepare for utility customers to ask more difficult questions about how a compromise on your end would be detected and contained.
- ✓ Consider independent certification to demonstrate security maturity beyond your own assurances.

Bottom Line

This month's incidents show that concentrated, shared infrastructure, vendors, credentials, and management consoles are now the primary targets, and AI is making those attacks faster and harder to predict. Utilities and suppliers who can verify security independently, rather than relying on trust alone, will be best positioned as this pattern continues.

KALEN

VALIDATING TRUST ACROSS THE GRID

POWERED BY GRID FRAMEWORK

ABOUT KALEN™



KALEN™ helps utilities and suppliers validate trust across the grid through recognized cybersecurity certifications, industry collaboration, and the GRID Framework.

By connecting utilities with suppliers that have demonstrated cybersecurity maturity through recognized validation mechanisms, KALEN™ supports more informed risk-management decisions and strengthens the resilience of critical infrastructure ecosystems.

FOR MORE INFORMATION

Visit **utc.org/KALEN** or contact Cordell Briggs.

VALIDATING TRUST ACROSS THE GRID. INFORMING WHAT COMES NEXT.

Utilities Technology Council™