Secora consulting

CISA KEV CATALOGUE

Vulnerability Watchlist Report

22 Jun 2026 – 28 Jun 2026

WINDOW	22 Jun 2026 – 28 Jun 2026
REPORT DATE	29 Jun 2026
CONTACT	sales@secoraconsulting.com

CONTENTS

Inside this report

1

Executive summary

A high-level overview of last week's threat landscape, highlighting top-priority risks and critical vulnerabilities. Designed for quick review by leadership and non-technical stakeholders.

1 Executive summary

A snapshot of this week's most critical threats, including a severity breakdown and our top remediation priorities.

WEEK ENDING 28 JUN 2026

6 CVES added

vs a 13-week average of 5.8, about an average week.

13 WEEKS

OVERALL RISK RATING

Critical

Immediate, severe risk. Patch now.

6 ACTIONABLE

Critical	5
High	1
Medium	0
Low	0
Unrated	0

This report covers the 6 vulnerabilities added to the CISA Known Exploited Vulnerabilities catalogue between 22 Jun 2026 and 28 Jun 2026. Of these, 6 are rated Critical or High and warrant priority remediation. CVE-2026-34910 ranks highest for modelled exploitation (99.5% EPSS percentile).

AFFECTED VENDORS

Ubiquiti 3 | Cisco 1 | Lantronix 1 | PTC 1

HIGHEST PRIORITY

Vulnerabilities that most warrant attention

10.0 CVSS **CRITICAL** CVE-2026-34910 01

Ubiquiti UniFi OS Improper Input Validation Vulnerability

Ubiquiti UniFi OS contains an improper input validation vulnerability which could allow ...

Read more →

10.0 CVSS **CRITICAL** CVE-2026-34908 02

Ubiquiti UniFi OS Improper Access Control Vulnerability

Ubiquiti UniFi OS contains an improper access control vulnerability which could allow ...

Read more →

10.0 CVSS **CRITICAL** CVE-2026-34909 03

Ubiquiti UniFi OS Path Traversal Vulnerability

Ubiquiti UniFi OS contains a path traversal vulnerability which could allow a malicious actor...

Read more →

2

Vulnerability dashboard

A consolidated view of all identified vulnerabilities, ranked by urgency. Review the full scope of required patching before diving into the technical details.

2 Vulnerability dashboard

A high-level summary of all findings, prioritized to streamline your initial triage.

SEVERITY	CVE	VENDOR / PRODUCT	VULNERABILITY	REMEDIATE BY
CRITICAL	CVE-2026-34910	Ubiquiti · UniFi OS	Ubiquiti UniFi OS Improper Input Validation Vulnerability	26 Jun 2026
CRITICAL	CVE-2026-34908	Ubiquiti · UniFi OS	Ubiquiti UniFi OS Improper Access Control Vulnerability	26 Jun 2026
CRITICAL	CVE-2026-34909	Ubiquiti · UniFi OS	Ubiquiti UniFi OS Path Traversal Vulnerability	26 Jun 2026
CRITICAL	CVE-2025-67038	Lantronix · EDS5000	Lantronix EDS5000 Code Injection Vulnerability	26 Jun 2026
CRITICAL	CVE-2026-12569	PTC · Windchill and FlexPLM	PTC Windchill and FlexPLM Improper Input Validation Vulnerability	28 Jun 2026
HIGH	CVE-2026-20230	Cisco · Unified Communications Manager	Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability	28 Jun 2026

3

Ranked vulnerabilities

An in-depth analysis of each finding. This section breaks down exploit mechanics, impact scoring (CVSS and EPSS), strict remediation deadlines, and the specific vendor advisories you need to act on.

3 Ranked vulnerabilities

Comprehensive technical details for each vulnerability, ordered from most to least critical to guide your immediate patching strategy.

3.1 Ubiquiti UniFi OS Improper Input Validation Vulnerability

▲ CRITICAL

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-34910 Added 23 Jun 2026	10.0/10 CRITICAL LOW MED HIGH CRIT	78.55% PROBABILITY 100th percentile (Top 1%) 0 DECILES 100%	26 Jun 2026 OVERDUE BY 3 DAYS Correct as of 29 Jun 2026

HOW IT'S EXPLOITED

ATTACK VECTOR	Network	COMPLEXITY	Low
PRIVILEGES	None	USER INTERACTION	None
SCOPE	Changed		

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	High	High

WHAT IT IS

Ubiquiti UniFi OS contains an improper input validation vulnerability which could allow a malicious actor with access to the network to conduct command injection.

RECOMMENDED ACTION

⚠ ACT NOW

Patch Ubiquiti UniFi OS to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Driven by top-1% exploit likelihood, critical severity and a missed CISA deadline.

WEAKNESS TYPE

CWE-20
Improper Input Validation

REFERENCES & ADVISORIES

Vendor advisory	https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-34910

3.2 Ubiquiti UniFi OS Improper Access Control Vulnerability

▲ CRITICAL

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-34908 Added 23 Jun 2026	**10.0**/10 CRITICAL LOW MED HIGH CRIT	**2.45%** PROBABILITY 82nd percentile (Top 50%) 0 DECILES 100%	26 Jun 2026 OVERDUE BY 3 DAYS Correct as of 29 Jun 2026

HOW IT'S EXPLOITED

ATTACK VECTOR	Network	COMPLEXITY	Low
PRIVILEGES	None	USER INTERACTION	None
SCOPE	Changed		

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	High	High

WHAT IT IS

Ubiquiti UniFi OS contains an improper access control vulnerability which could allow a malicious actor with access to the network to make unauthorized changes to the system.

RECOMMENDED ACTION

⚠ ACT NOW

Patch Ubiquiti UniFi OS to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Driven by critical severity and a missed CISA deadline.

WEAKNESS TYPE

CWE-284
Improper Access Control

REFERENCES & ADVISORIES

Vendor advisory	https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-34908

3.3 Ubiquiti UniFi OS Path Traversal Vulnerability

▲ CRITICAL

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-34909 Added 23 Jun 2026	**10.0**/10 CRITICAL LOW MED HIGH CRIT	**2.27%** PROBABILITY 81st percentile (Top 50%) 0 DECILES 100%	26 Jun 2026 OVERDUE BY 3 DAYS Correct as of 29 Jun 2026

HOW IT'S EXPLOITED

ATTACK VECTOR	Network	COMPLEXITY	Low
PRIVILEGES	None	USER INTERACTION	None
SCOPE	Changed		

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	High	High

WHAT IT IS

Ubiquiti UniFi OS contains a path traversal vulnerability which could allow a malicious actor with access to the network to access files on the underlying system that could be manipulated to access an underlying account.

RECOMMENDED ACTION

⚠ ACT NOW

Patch Ubiquiti UniFi OS to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Driven by critical severity and a missed CISA deadline.

WEAKNESS TYPE

CWE-22
Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)

REFERENCES & ADVISORIES

Vendor advisory	https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-34909

3.4 Lantronix EDS5000 Code Injection Vulnerability

▲ CRITICAL

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2025-67038 Added 23 Jun 2026	9.8/10 CRITICAL LOW MED HIGH CRIT	1.13% PROBABILITY 62nd percentile (Top 50%) 0 DECILES 100%	26 Jun 2026 OVERDUE BY 3 DAYS Correct as of 29 Jun 2026

HOW IT'S EXPLOITED

ATTACK VECTOR	Network	COMPLEXITY	Low
PRIVILEGES	None	USER INTERACTION	None
SCOPE	Unchanged		

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	High	High

WHAT IT IS

Lantronix EDS5000 contains a code injection vulnerability that could allow attackers to inject arbitrary OS commands into the username parameter. Injected commands are executed with root privileges.

RECOMMENDED ACTION

⚠ ACT NOW

Patch Lantronix EDS5000 to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Driven by critical severity and a missed CISA deadline.

WEAKNESS TYPE

CWE-78
Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)

CWE-94
Improper Control of Generation of Code (Code Injection)

REFERENCES & ADVISORIES

ltrxdev.atlassian.net	https://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/pages/2538438657/Latest+Firmware+for+the+EDS5000+series+EDS5008+EDS5016+EDS5032
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-67038

3.5 PTC Windchill and FlexPLM Improper Input Validation Vulnerability

▲ CRITICAL

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-12569 Added 25 Jun 2026	9.8/10 CRITICAL LOW MED HIGH CRIT	1.11% PROBABILITY 62nd percentile (Top 50%) 0 DECILES 100%	28 Jun 2026 OVERDUE BY 1 DAY Correct as of 29 Jun 2026

HOW IT'S EXPLOITED

ATTACK VECTOR	Network	COMPLEXITY	Low
PRIVILEGES	None	USER INTERACTION	None
SCOPE	Unchanged		

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	High	High

WHAT IT IS

PTC Windchill and FlexPLM contains an improper input validation vulnerability allowing an unauthenticated, remote attacker to execute arbitrary code by sending a malicious request to the network.

RECOMMENDED ACTION

⚠ ACT NOW

Patch PTC Windchill and FlexPLM to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Driven by critical severity and a missed CISA deadline.

WEAKNESS TYPE

CWE-20
Improper Input Validation

CWE-502
Deserialization of Untrusted Data

REFERENCES & ADVISORIES

www.ptc.com	https://www.ptc.com/en/support/article/CS473270
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-12569

3.6 Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability

▲ HIGH

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-20230 Added 25 Jun 2026	8.6/10 HIGH LOW MED HIGH CRIT	41.69% PROBABILITY 99th percentile (Top 10%) 0 DECILES 100%	28 Jun 2026 OVERDUE BY 1 DAY Correct as of 29 Jun 2026

HOW IT'S EXPLOITED

ATTACK VECTOR	Network	COMPLEXITY	Low
PRIVILEGES	None	USER INTERACTION	None
SCOPE	Changed		

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
None	High	None

WHAT IT IS

Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) contain a server-side request forgery (SSRF) Vulnerability that could allow an unauthenticated, remote attacker to write files to the underlying operating system that could be used later to elevate to root.

RECOMMENDED ACTION ⚠ ACT NOW

Patch Cisco Unified Communications Manager to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Driven by top-10% exploit likelihood, high severity and a missed CISA deadline.

WEAKNESS TYPE

CWE-918
Server-Side Request Forgery (SSRF)

REFERENCES & ADVISORIES

Vendor advisory	https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-cucm-ssrf-cXPnHcW.html
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20230

4

Remediation roadmap

Your tactical action plan. This working checklist groups vulnerabilities by their CISA-mandated deadlines so you can immediately target overdue items.

4 Remediation roadmap

A deadline-driven checklist to help your team track and execute required security patches efficiently

Overdue: remediate immediately · 6

- **CVE-2026-34910: Ubiquiti UniFi OS Improper Input Validation Vulnerability**
  Patch Ubiquiti UniFi OS to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2026-34908: Ubiquiti UniFi OS Improper Access Control Vulnerability**
  Patch Ubiquiti UniFi OS to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2026-34909: Ubiquiti UniFi OS Path Traversal Vulnerability**
  Patch Ubiquiti UniFi OS to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2025-67038: Lantronix EDS5000 Code Injection Vulnerability**
  Patch Lantronix EDS5000 to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2026-12569: PTC Windchill and FlexPLM Improper Input Validation Vulnerability**
  Patch PTC Windchill and FlexPLM to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2026-20230: Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability**
  Patch Cisco Unified Communications Manager to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

5

Methodology & data sources

The framework behind our findings. This section outlines our intelligence sources, ranking methodology, and the scope of this report to provide necessary context.

5 Methodology & data sources

An overview of the data sources and scoring criteria used to compile and prioritize these vulnerabilities.

This report is compiled from the U.S. CISA Known Exploited Vulnerabilities (KEV) catalogue, filtered to vulnerabilities newly added between 22 Jun 2026 and 28 Jun 2026. Each entry is enriched with its NVD CVSS score and severity and its FIRST EPSS exploit-prediction percentile, then ranked so the highest-priority items appear first.

DATA SOURCES

- CISA Known Exploited Vulnerabilities Catalogue: authoritative list of CVEs with confirmed in-the-wild exploitation.
- NVD (National Vulnerability Database): CVSS base scores, severities and vectors.
- FIRST EPSS: Exploit Prediction Scoring System percentiles indicating relative exploitation likelihood.

HOW WE RANK

- Known ransomware-campaign use is surfaced first as the sharpest signal of active exploitation.
- CVSS severity and base score weight the technical impact of each vulnerability.
- When two vulnerabilities are equally severe, the one EPSS rates as more likely to be exploited is ranked higher.
- CISA-assigned due dates flag the remediation deadlines that apply to federal agencies.

LIMITATIONS

The KEV catalogue lists vulnerabilities confirmed as exploited; absence from it is not evidence of safety. This report does not assess whether the affected products are present in your environment. Use it to prioritise patching against your own asset inventory.

6

Next steps

Turn these insights into action. Discover how Secora Consulting can support your remediation efforts and connect with our team.

6 Next steps

Ready to secure your environment? Here is how our team can help you navigate and resolve these vulnerabilities.

Penetration Testing

A hands-on, authorised attack against your live systems to prove which of these exposures an attacker could actually reach and exploit in your environment.

Vulnerability Assessments

A structured, authenticated sweep of your infrastructure and applications to find and prioritise the weaknesses behind the CVEs in this report.

Adversary Simulation Testing

A real-world attack scenario that tests your detection and response, not just your defences. It shows how far a determined attacker gets before you stop them.

Simulated Phishing Attacks

Controlled phishing against your team to measure and build real resistance to the social-engineering techniques that so often precede exploitation.

Need help remediating these vulnerabilities?

Our team can help you prioritise and patch the vulnerabilities in this report. Get in touch for a free consultation.

Get a free consultation →

7

About Secora Consulting

Who we are, why organisations choose us, and the accreditations and qualifications that stand behind this report.

7 About Secora Consulting

Who we are and why organisations trust us with their security.

Secora Consulting is an Irish cybersecurity consultancy specialising in penetration testing, vulnerability assessment and security advisory. We help organisations of every size understand their real-world exposure and act on it with clear, prioritised, business-focused advice, not just a list of findings.

WHY CHOOSE US

- **Certified, experienced consultants:** Our team holds industry-recognised certifications and brings years of hands-on offensive and defensive security experience.
- **Clear, actionable reporting:** Every finding comes with practical, prioritised remediation guidance written for both technical teams and leadership.
- **Independent and vendor-neutral:** We sell no products, so our recommendations serve only your security, never a sales agenda.
- **A partner, not a one-off supplier:** We work alongside your team before, during and after testing to make sure issues actually get fixed.

COMPANY ACCREDITATIONS

CREST PEN TEST

Donegal Enterprise Awards 2021 BEST ESTABLISHED BUSINESS WINNER

AMTIVO ISO 9001 Certified Quality Management

AMTIVO ISO 27001 Certified Information Security Management

CONSULTANT QUALIFICATIONS

CERTIFIED RED TEAM PROFESSIONAL · WINDOWS RED TEAMING EXPERT · CISA · CISM · OFFENSIVE OSWP · CIPP · CPSA · CRT · OFFENSIVE OSCP · WAPT · AZURE FUNDAMENTALS · ECSS · ITIL V3 Certified · (CESP - ADCS) · Burp Suite Certified PRACTITIONER · PCI Qualified Security Assessor (QSA) · Certified EU GDPR Foundation C GDPR F · COBIT · EC-Council CEH MASTER CERTIFIED

A

Understanding KEV, CVSS & EPSS

A plain-language guide to the three data sources behind this report, and what each one tells you.

APPENDIX A

A Understanding the data

Three independent sources sit behind every finding in this report. Each answers a different question.

CISA KEV: the Known Exploited Vulnerabilities Catalogue

The KEV catalogue is a list, published and maintained by the United States Cybersecurity and Infrastructure Security Agency (CISA), of software vulnerabilities that are known to have been actively exploited by attackers in the real world. A vulnerability earns a place on the list only once there is reliable evidence it has been used in an attack, which makes inclusion one of the strongest available signals that a flaw is worth fixing quickly. Every vulnerability in this report is drawn from that catalogue.

CVSS: how severe a vulnerability is

The Common Vulnerability Scoring System is an open, industry-standard way of rating how serious a vulnerability is, on a scale from 0 to 10. The score is calculated from the characteristics of the flaw itself, such as whether it can be exploited over the internet, how much skill or access an attacker needs, and how much damage a successful attack could cause. Broadly, 0.1 to 3.9 is Low, 4.0 to 6.9 is Medium, 7.0 to 8.9 is High, and 9.0 to 10.0 is Critical. A higher score means a more dangerous flaw.

EPSS: how likely exploitation is

The Exploit Prediction Scoring System, maintained by FIRST, estimates how likely a vulnerability is to be exploited in the near future. Where CVSS measures how bad a flaw would be if it were exploited, EPSS estimates how probable that exploitation actually is, expressed as a percentile from 0 to 100%. A vulnerability in the top few percent is among the most likely to be attacked. We read EPSS alongside CVSS so that effort goes first to the flaws that are both serious and likely to be used.

Used together, these three sources answer different questions. The KEV catalogue confirms a vulnerability is being exploited, CVSS describes how damaging it could be, and EPSS estimates how likely exploitation is. Reading them side by side is what lets this report rank the findings by genuine priority rather than severity alone.