Secora consulting

CISA KEV CATALOGUE

Vulnerability Watchlist Report

8 Jun 2026 – 14 Jun 2026

WINDOW	8 Jun 2026 – 14 Jun 2026
REPORT DATE	15 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 14 JUN 2026

7 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	3
High	3
Medium	1
Low	0
Unrated	0

This report covers the 7 vulnerabilities added to the CISA Known Exploited Vulnerabilities catalogue between 8 Jun 2026 and 14 Jun 2026. Of these, 6 are rated Critical or High and warrant priority remediation, and 2 are linked to known ransomware campaigns. CVE-2026-42271 ranks highest for modelled exploitation (98.3% EPSS percentile).

AFFECTED VENDORS

Arista 1 | BerriAI 1 | Check Point 1 | Cisco 1 | Google 1 | Ivanti 1 | Oracle 1

HIGHEST PRIORITY

Vulnerabilities that most warrant attention

01

9.8 CVSS **CRITICAL** CVE-2026-35273

Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability

Oracle PeopleSoft Enterprise PeopleTools contains a missing authentication for critical...

Read more →

02

9.3 CVSS **CRITICAL** CVE-2026-50751

Check Point Security Gateway Improper Authentication Vulnerability

Check Point Security Gateway contains an improper authentication vulnerability in...

Read more →

03

10.0 CVSS **CRITICAL** CVE-2026-10520

Ivanti Sentry OS Command Injection Vulnerability

Ivanti Sentry (formerly known as MobileIron Sentry) contains an OS command injection...

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-2026-35273 RANSOMWARE	Oracle · PeopleSoft Enterprise PeopleTools	Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability	15 Jun 2026
CRITICAL	CVE-2026-50751 RANSOMWARE	Check Point · Security Gateway	Check Point Security Gateway Improper Authentication Vulnerability	11 Jun 2026
CRITICAL	CVE-2026-10520	Ivanti · Sentry	Ivanti Sentry OS Command Injection Vulnerability	14 Jun 2026
HIGH	CVE-2026-42271	BerriAI · LiteLLM	BerriAI LiteLLM Command Injection Vulnerability	22 Jun 2026
HIGH	CVE-2026-11645	Google · Chromium V8	Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	23 Jun 2026
HIGH	CVE-2026-20245	Cisco · Catalyst SD-WAN Manager	Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability	23 Jun 2026
MEDIUM	CVE-2026-7473	Arista · Extensible Operating System	Arista Extensible Operating System Incomplete Comparison with Missing Factors Vulnerability	23 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 Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability

RANSOMWARE ▲ CRITICAL

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-35273 Added 12 Jun 2026	9.8/10 CRITICAL LOW MED HIGH CRIT	19.82% PROBABILITY 96th percentile (Top 10%) 0 DECILES 100%	15 Jun 2026 DUE TODAY Correct as of 15 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

Oracle PeopleSoft Enterprise PeopleTools contains a missing authentication for critical function vulnerability which could allow an unauthenticated attacker to obtain takeover of PeopleSoft Enterprise PeopleTools.

RECOMMENDED ACTION ⚠ ACT NOW

Patch Oracle PeopleSoft Enterprise PeopleTools to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Driven by active ransomware use, top-10% exploit likelihood and critical severity.

WEAKNESS TYPE

CWE-306
Missing Authentication for Critical Function

REFERENCES & ADVISORIES

Vendor advisory	https://www.oracle.com/security-alerts/alert-cve-2026-35273.html
Vendor advisory	https://support.oracle.com/signin/
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-35273

3.2 Check Point Security Gateway Improper Authentication Vulnerability

RANSOMWARE ▲ CRITICAL

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-50751 Added 8 Jun 2026	9.3/10 CRITICAL LOW MED HIGH CRIT	13.73% PROBABILITY 94th percentile (Top 10%) 0 DECILES 100%	11 Jun 2026 OVERDUE BY 4 DAYS Correct as of 15 Jun 2026

HOW IT'S EXPLOITED

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

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	Low	None

WHAT IT IS

Check Point Security Gateway contains an improper authentication vulnerability in IKEv1 key exchange that could allow an unauthenticated remote attacker to bypass user authentication and establish a remote access VPN connection without a valid user password.

RECOMMENDED ACTION

⚠ ACT NOW

Patch Check Point Security Gateway to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Driven by active ransomware use, top-10% exploit likelihood, critical severity and a missed CISA deadline.

WEAKNESS TYPE

CWE-287
Improper Authentication

REFERENCES & ADVISORIES

Patch / release notes	https://blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol/
support.checkpoint.com	https://support.checkpoint.com/results/sk/sk185033?_gl=1*1wqeqhc*_gcl_au*MTI1MzE5MjI2LjE3ODA5MzQ1NTM
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-50751

3.3 Ivanti Sentry OS Command Injection Vulnerability

▲ CRITICAL

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-10520 Added 11 Jun 2026	**10.0**/10 CRITICAL LOW MED HIGH CRIT	**42.70%** PROBABILITY 98th percentile (Top 10%) 0 DECILES 100%	14 Jun 2026 OVERDUE BY 1 DAY Correct as of 15 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

Ivanti Sentry (formerly known as MobileIron Sentry) contains an OS command injection vulnerability which could allow a remote unauthenticated user to achieve root-level remote code execution. This vulnerability can be successfully exploited in cases where the Sentry appliance is in an unmanaged state with its endpoints externally reachable. The use of mTLS with EPMM or restricted HTTPS access through Neurons for MDM makes interfaces inaccessible to external actors.

RECOMMENDED ACTION

⚠ ACT NOW

Patch Ivanti Sentry 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, critical severity and a missed CISA deadline.

WEAKNESS TYPE

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

REFERENCES & ADVISORIES

Vendor advisory	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523?language=en_US
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-10520

3.4 BerriAI LiteLLM Command Injection Vulnerability

▲ HIGH

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-42271 Added 8 Jun 2026	**8.8**/10 HIGH LOW MED HIGH CRIT	**60.78%** PROBABILITY 98th percentile (Top 10%) 0 DECILES 100%	22 Jun 2026 DUE IN 7 DAYS Correct as of 15 Jun 2026

HOW IT'S EXPLOITED

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

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	High	High

WHAT IT IS

BerriAI LiteLLM contains a command injection vulnerability that could allow any authenticated user, including holders of low-privilege internal-user keys, to run arbitrary commands on the host.

RECOMMENDED ACTION

⚠ ACT NOW

Patch BerriAI LiteLLM 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 and high severity.

WEAKNESS TYPE

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

CWE-77
Improper Neutralization of Special Elements used in a Command (Command Injection)

REFERENCES & ADVISORIES

github.com	https://github.com/BerriAI/litellm/releases/tag/v1.83.7-stable
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-42271

3.5 Google Chromium V8 Out-of-Bounds Read and Write Vulnerability

▲ HIGH

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-11645 Added 9 Jun 2026	**8.8**/10 HIGH LOW MED HIGH CRIT	**5.89%** PROBABILITY 91st percentile (Top 10%) 0 DECILES 100%	23 Jun 2026 DUE IN 8 DAYS Correct as of 15 Jun 2026

HOW IT'S EXPLOITED

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

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	High	High

WHAT IT IS

Google Chromium V8 out-of-bounds read and write vulnerability that could allow a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. This vulnerability could affect multiple web browsers that utilize Chromium, including, but not limited to, Google Chrome, Microsoft Edge, and Opera.

RECOMMENDED ACTION

⚠ PRIORITISE

Patch Google Chromium V8 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 and high severity.

WEAKNESS TYPE

CWE-787
Out-of-bounds Write

CWE-125
Out-of-bounds Read

REFERENCES & ADVISORIES

Patch / release notes	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
issues.chromium.org	https://issues.chromium.org/issues/506689381
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-11645

3.6 Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability

▲ HIGH

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-20245 Added 9 Jun 2026	7.8/10 HIGH LOW MED HIGH CRIT	0.36% PROBABILITY 58th percentile (Top 50%) 0 DECILES 100%	23 Jun 2026 DUE IN 8 DAYS Correct as of 15 Jun 2026

HOW IT'S EXPLOITED

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

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	High	High

WHAT IT IS

Cisco Catalyst SD-WAN Manager formerly SD-WAN vManage contains an improper encoding or escaping of output vulnerability. This vulnerability could allow an authenticated, local attacker to execute arbitrary commands as root by supplying a crafted file to the affected system.

RECOMMENDED ACTION ⚠ PRIORITISE

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

Driven by high severity.

WEAKNESS TYPE

CWE-116
Improper Encoding or Escaping of Output

REFERENCES & ADVISORIES

Vendor advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20245

3.7 Arista Extensible Operating System Incomplete Comparison with Missing Factors Vulnerability

▲ MEDIUM

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-7473 Added 9 Jun 2026	5.8/10 MEDIUM LOW MED HIGH CRIT	27.22% PROBABILITY 97th percentile (Top 10%) 0 DECILES 100%	23 Jun 2026 DUE IN 8 DAYS Correct as of 15 Jun 2026

HOW IT'S EXPLOITED

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

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
None	Low	None

WHAT IT IS

Arista Extensible Operating System (EOS) contains an incomplete comparison with missing factors vulnerability when the switch incorrectly decapsulate and forwards other unexpected tunneled packet with a destination IP matching its configured decapsulation IP.

RECOMMENDED ACTION ⚠ PRIORITISE

Patch Arista Extensible Operating System 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.

WEAKNESS TYPE

CWE-1023

REFERENCES & ADVISORIES

Vendor advisory	https://www.arista.com/en/support/advisories-notices/security-advisory/24005-security-advisory-0137
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-7473

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 · 2

- **CVE-2026-50751: Check Point Security Gateway Improper Authentication Vulnerability**
  Patch Check Point Security Gateway to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2026-10520: Ivanti Sentry OS Command Injection Vulnerability**
  Patch Ivanti Sentry to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Due within 7 days · 2

- **CVE-2026-35273: Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability**
  Patch Oracle PeopleSoft Enterprise PeopleTools to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2026-42271: BerriAI LiteLLM Command Injection Vulnerability**
  Patch BerriAI LiteLLM to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Due within 14 days · 3

- **CVE-2026-11645: Google Chromium V8 Out-of-Bounds Read and Write Vulnerability**
  Patch Google Chromium V8 to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2026-20245: Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability**
  Patch Cisco Catalyst SD-WAN Manager to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2026-7473: Arista Extensible Operating System Incomplete Comparison with Missing Factors Vulnerability**
  Patch Arista Extensible Operating System 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 8 Jun 2026 and 14 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.