Secora consulting

CISA KEV CATALOGUE

Vulnerability Watchlist Report

1 Jun 2026 – 7 Jun 2026

WINDOW	1 Jun 2026 – 7 Jun 2026
REPORT DATE	8 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 7 JUN 2026

5 CVES added

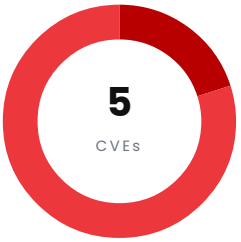
vs a 13-week average of 5.9, about an average week.

13 WEEKS

OVERALL RISK RATING

Critical

Immediate, severe risk. Patch now.



5 ACTIONABLE

Critical	1
High	4
Medium	0
Low	0
Unrated	0

This report covers the 5 vulnerabilities added to the CISA Known Exploited Vulnerabilities catalogue between 1 Jun 2026 and 7 Jun 2026. Of these, 5 are rated Critical or High and warrant priority remediation. CVE-2024-21182 ranks highest for modelled exploitation (99.6% EPSS percentile).

AFFECTED VENDORS

Android 1 | Linux 1 | Mirasvit 1 | Oracle 1 | SolarWinds 1

HIGHEST PRIORITY

Vulnerabilities that most warrant attention

01

9.8 CVSS **CRITICAL** CVE-2026-45247

Mirasvit Full Page Cache Warmer Deserialization of Untrusted Data Vulnerability

Mirasvit Full Page Cache Warmer contains a deserialization of untrusted data vulnerability that could allow unauthenticated attackers to achieve remote code execution by supplying a crafted serialized PHP object in the CacheWarmer cookie.

02

7.5 CVSS **HIGH** CVE-2024-21182

Oracle WebLogic Server Unspecified Vulnerability

Oracle WebLogic contains an unspecified vulnerability that could allow an unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data.

03

7.8 CVSS **HIGH** CVE-2022-0492

Linux Kernel Improper Authentication Vulnerability

Linux Kernel contains an improper authentication vulnerability which could allow for privilege escalation via the cgroups v1 release_agent feature.

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-2026-45247	Mirasvit · Mirasvit Full Page Cache Warmer	Mirasvit Full Page Cache Warmer Deserialization of Untrusted Data Vulnerability	6 Jun 2026
HIGH	CVE-2024-21182	Oracle · WebLogic Server	Oracle WebLogic Server Unspecified Vulnerability	4 Jun 2026
HIGH	CVE-2022-0492	Linux · Kernel	Linux Kernel Improper Authentication Vulnerability	5 Jun 2026
HIGH	CVE-2026-28318	SolarWinds · Serv-U	SolarWinds Serv-U Uncontrolled Resource Consumption Vulnerability	19 Jun 2026
HIGH	CVE-2025-48595	Android · Framework	Android Framework Integer Overflow Vulnerability	5 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 Mirasvit Full Page Cache Warmer Deserialization of Untrusted Data Vulnerability

▲ CRITICAL

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-45247 Added 3 Jun 2026	9.8/10 CRITICAL LOW MED HIGH CRIT	6.15% PROBABILITY 91st percentile (Top 10%) 0 DECILES 100%	6 Jun 2026 OVERDUE BY 2 DAYS Correct as of 8 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

Mirasvit Full Page Cache Warmer contains a deserialization of untrusted data vulnerability that could allow unauthenticated attackers to achieve remote code execution by supplying a crafted serialized PHP object in the CacheWarmer cookie.

RECOMMENDED ACTION

⚠ ACT NOW

Patch Mirasvit Full Page Cache Warmer 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-502
Deserialization of Untrusted Data

REFERENCES & ADVISORIES

mirasvit.com	https://mirasvit.com/package/changelog/?package=mirasvit/module-cache-warmer
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-45247

3.2 Oracle WebLogic Server Unspecified Vulnerability

▲ HIGH

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2024-21182 Added 1 Jun 2026	**7.5**/10 HIGH LOW MED HIGH CRIT	**89.65%** PROBABILITY 100th percentile (Top 1%) 0 DECILES 100%	4 Jun 2026 OVERDUE BY 4 DAYS Correct as of 8 Jun 2026

HOW IT'S EXPLOITED

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

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	None	None

WHAT IT IS

Oracle WebLogic contains an unspecified vulnerability that could allow an unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data.

RECOMMENDED ACTION

⚠ ACT NOW

Patch Oracle WebLogic Server 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, high severity and a missed CISA deadline.

WEAKNESS TYPE

N/A

REFERENCES & ADVISORIES

Vendor advisory	https://www.oracle.com/security-alerts/cpujul2024.html
NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-21182

3.3 Linux Kernel Improper Authentication Vulnerability

▲ HIGH

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2022-0492 Added 2 Jun 2026	**7.8**/10 HIGH LOW MED HIGH CRIT	**28.12%** PROBABILITY 97th percentile (Top 10%) 0 DECILES 100%	5 Jun 2026 OVERDUE BY 3 DAYS Correct as of 8 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

Linux Kernel contains an improper authentication vulnerability which could allow for privilege escalation via the cgroups v1 release_agent feature.

RECOMMENDED ACTION

⚠ ACT NOW

Patch Linux Kernel 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-287
Improper Authentication

CWE-862
Missing Authorization

REFERENCES & ADVISORIES

www.kernel.org	https://www.kernel.org/
NVD	https://nvd.nist.gov/vuln/detail/CVE-2022-0492

3.4 SolarWinds Serv-U Uncontrolled Resource Consumption Vulnerability

▲ HIGH

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2026-28318 Added 5 Jun 2026	7.5/10 HIGH LOW MED HIGH CRIT	6.68% PROBABILITY 91st percentile (Top 10%) 0 DECILES 100%	19 Jun 2026 DUE IN 11 DAYS Correct as of 8 Jun 2026

HOW IT'S EXPLOITED

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

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
None	None	High

WHAT IT IS

SolarWinds Serv-U contains an uncontrolled resource consumption vulnerability that allows specially crafted POST requests using the Content-Encoding: deflate header to crash the Serv-U service without authentication.

RECOMMENDED ACTION

⚠ PRIORITISE

Patch SolarWinds Serv-U 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-400
Uncontrolled Resource Consumption

REFERENCES & ADVISORIES

Vendor advisory	https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28318
Patch / release notes	https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_15-5-4-hotfix-1_release_notes.htm#link7
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-28318

3.5 Android Framework Integer Overflow Vulnerability

▲ HIGH

CVE	CVSS BASE	EXPLOIT LIKELIHOOD (EPSS)	REMEDIATE BY
CVE-2025-48595 Added 2 Jun 2026	**8.4**/10 HIGH LOW MED HIGH CRIT	**0.53%** PROBABILITY 68th percentile (Top 50%) 0 DECILES 100%	5 Jun 2026 OVERDUE BY 3 DAYS Correct as of 8 Jun 2026

HOW IT'S EXPLOITED

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

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	High	High

WHAT IT IS

Android Framework contains an integer overflow vulnerability that allows for code execution that could allow for local privilege escalation.

RECOMMENDED ACTION

⚠ ACT NOW

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

Driven by high severity and a missed CISA deadline.

WEAKNESS TYPE

CWE-190
Integer Overflow or Wraparound

REFERENCES & ADVISORIES

Vendor advisory	https://source.android.com/docs/security/bulletin/2026/2026-06-01
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-48595

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 · 4

- **CVE-2026-45247: Mirasvit Full Page Cache Warmer Deserialization of Untrusted Data Vulnerability**
  Patch Mirasvit Full Page Cache Warmer to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2024-21182: Oracle WebLogic Server Unspecified Vulnerability**
  Patch Oracle WebLogic Server to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2022-0492: Linux Kernel Improper Authentication Vulnerability**
  Patch Linux Kernel to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2025-48595: Android Framework Integer Overflow Vulnerability**
  Patch Android Framework to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Due within 14 days · 1

- **CVE-2026-28318: SolarWinds Serv-U Uncontrolled Resource Consumption Vulnerability**
  Patch SolarWinds Serv-U 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 1 Jun 2026 and 7 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.