



Secora
consulting

CISA KEV CATALOGUE

Vulnerability Watchlist Report

15 Jun 2026 - 21 Jun 2026

WINDOW

15 Jun 2026 - 21 Jun 2026

REPORT DATE

22 Jun 2026

CONTACT

sales@secoraconsulting.com

CONTENTS

Inside this report

1	Executive summary	2
2	Vulnerability dashboard	4
3	Ranked vulnerabilities	6
4	Remediation roadmap	11
5	Methodology & data sources	13
6	Next steps	15
7	About Secora Consulting	17
A	Understanding KEV, CVSS & EPSS	19

IMPORTANT NOTICE

This report is provided by Secora Consulting for information purposes only and reflects the CISA KEV catalogue and associated data as it stood for the period 15 Jun 2026 and 21 Jun 2026. The threat landscape changes continually, so entries, scores and remediation deadlines may have changed since publication.

It is compiled from third-party sources (CISA, the NVD and FIRST EPSS) and its accuracy depends on those sources. The KEV catalogue lists only vulnerabilities confirmed as exploited; it is not a complete inventory of your exposure, and absence from it is not evidence of safety. This report does not assess whether the affected products are present in your environment and is not a substitute for a tailored security assessment.

Acting on this report does not guarantee security against compromise. Secora Consulting accepts no liability for loss or damage arising from reliance on it; recommendations should be prioritised against your own asset inventory and risk context.

Links to vendor advisories and other third-party sources are provided for convenience only. Secora Consulting does not control that content and cannot guarantee its accuracy or availability; always obtain patches and guidance directly from the vendor and verify their authenticity before acting.



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 21 JUN 2026

4 CVEs added
vs a 13-week average of 5.7, a lighter-than-usual week.

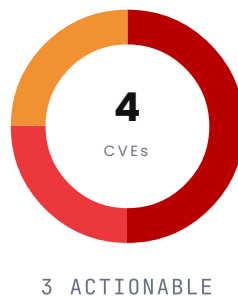


13 WEEKS

OVERALL RISK RATING

Critical

Immediate, severe risk. Patch now.



Critical	2
High	1
Medium	1
Low	0
Unrated	0

This report covers the 4 vulnerabilities added to the CISA Known Exploited Vulnerabilities catalogue between 15 Jun 2026 and 21 Jun 2026. Of these, 3 are rated Critical or High and warrant priority remediation. CVE-2026-20253 ranks highest for modelled exploitation (95.0% EPSS percentile).

AFFECTED VENDORS

Cisco **1** LiteSpeed **1** Splunk **1** Widget Factory **1**

HIGHEST PRIORITY

Vulnerabilities that most warrant attention

9.8 **CRITICAL** 01
CVSS CVE-2026-20253

Splunk Enterprise Missing Authentication for Critical Function Vulnerability

Splunk Enterprise contains a missing authentication for critical function vulnerability which coul...

[Read more →](#)

9.8 **CRITICAL** 02
CVSS CVE-2026-48907

Widget Factory Joomla Content Editor Improper Access Control Vulnerability

Widget Factory Joomla Content Editor contains an improper access control vulnerability...

[Read more →](#)

8.5 **HIGH** 03
CVSS CVE-2026-54420

LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability

LiteSpeed cPanel plugin contains a UNIX symbolic link (Symlink) following vulnerability that coul...

[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-2026-20253	Splunk · Enterprise	Splunk Enterprise Missing Authentication for Critical Function Vulnerability	21 Jun 2026
CRITICAL	CVE-2026-48907	Widget Factory · Joomla Content Editor	Widget Factory Joomla Content Editor Improper Access Control Vulnerability	19 Jun 2026
HIGH	CVE-2026-54420	LiteSpeed · cPanel Plugin	LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability	18 Jun 2026
MEDIUM	CVE-2026-20262	Cisco · Catalyst SD-WAN Manager	Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability	29 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 Splunk Enterprise Missing Authentication for Critical Function Vulnerability

▲ CRITICAL

CVE CVE-2026-20253 Added 18 Jun 2026	CVSS BASE 9.8/10 CRITICAL 	EXPLOIT LIKELIHOOD (EPSS) 10.04% PROBABILITY 95th percentile (Top 10%) 	REMEDIATE BY 21 Jun 2026 OVERDUE BY 1 DAY Correct as of 22 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

Splunk Enterprise contains a missing authentication for critical function vulnerability which could allow an unauthenticated user to create or truncate arbitrary files through a PostgreSQL sidecar service endpoint.

RECOMMENDED ACTION

▲ ACT NOW

Patch Splunk Enterprise 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-306
Missing Authentication for Critical Function

REFERENCES & ADVISORIES

Vendor advisory	https://advisory.splunk.com/advisories/SVD-2026-0603
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20253

3.2 Widget Factory Joomla Content Editor Improper Access Control Vulnerability

▲ CRITICAL

<p>CVE</p> <p>CVE-2026-48907</p> <p>Added 16 Jun 2026</p>	<p>CVSS BASE</p> <p>9.8/10 CRITICAL</p> <p>LOW MED HIGH CRIT</p>	<p>EXPLOIT LIKELIHOOD (EPSS)</p> <p>6.85% PROBABILITY</p> <p>93rd percentile (Top 10%)</p> <p>0 DECILES 100%</p>	<p>REMEDIATE BY</p> <p>19 Jun 2026</p> <p>OVERDUE BY 3 DAYS</p> <p>Correct as of 22 Jun 2026</p>
--	--	--	--

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

Widget Factory Joomla Content Editor contains an improper access control vulnerability which could allow for upload and execution of PHP code via the creation of new editor profiles for unauthenticated users.

RECOMMENDED ACTION

▲ ACT NOW

Patch Widget Factory Joomla Content Editor 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-284
Improper Access Control

REFERENCES & ADVISORIES

Patch / release notes	https://www.joomlacontenteditor.net/news/jce-security-update-and-a-free-patch-for-older-sites
www.joomlacontenteditor.net	https://www.joomlacontenteditor.net/support/changeLog/editor
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-48907

3.3 LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability

▲ HIGH

CVE CVE-2026-54420 Added 15 Jun 2026	CVSS BASE 8.5/10 HIGH 	EXPLOIT LIKELIHOOD (EPSS) 0.65% PROBABILITY 46th percentile (Lower half) 	REMEDIATE BY 18 Jun 2026 OVERDUE BY 4 DAYS Correct as of 22 Jun 2026
---	--	--	---

HOW IT'S EXPLOITED

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

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
High	High	High

WHAT IT IS

LiteSpeed cPanel plugin contains a UNIX symbolic link (Symlink) following vulnerability that could allow a user with FTP or web shell access on a shared hosting server running CloudLinux/CageFS.

RECOMMENDED ACTION **▲ ACT NOW**

Patch LiteSpeed cPanel Plugin 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-61

REFERENCES & ADVISORIES

blog.litespeedtech.com	https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-54420

3.4 Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability

▲ MEDIUM

CVE CVE-2026-20262 Added 15 Jun 2026	CVSS BASE 6.5/10 MEDIUM 	EXPLOIT LIKELIHOOD (EPSS) 1.15% PROBABILITY 63rd percentile (Top 50%) 	REMEDIATE BY 29 Jun 2026 DUE IN 7 DAYS Correct as of 22 Jun 2026
---	--	---	---

HOW IT'S EXPLOITED

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

IMPACT

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
None	High	None

WHAT IT IS

Cisco Catalyst SD-WAN Manager contains a directory or path traversal vulnerability that could allow an authenticated, remote attacker to create a file or overwrite any file on the filesystem of an affected system.

RECOMMENDED ACTION

⚠ SCHEDULE

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.

WEAKNESS TYPE

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

REFERENCES & ADVISORIES

Vendor advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20262

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 · 3

- **CVE-2026-20253: Splunk Enterprise Missing Authentication for Critical Function Vulnerability**
Patch Splunk Enterprise to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2026-48907: Widget Factory Joomla Content Editor Improper Access Control Vulnerability**
Patch Widget Factory Joomla Content Editor to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.
- **CVE-2026-54420: LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability**
Patch LiteSpeed cPanel Plugin to the vendor's fixed release; if none is available, apply the published mitigations or remove it from service.

Due within 7 days · 1

- **CVE-2026-20262: Cisco Catalyst SD-WAN Manager Directory or Path Traversal 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.

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 15 Jun 2026 and 21 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



CONSULTANT QUALIFICATIONS





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.

