Top 15 Web-Based CVEs (September–November 2025): Research Report

Executive Summary

The three-month period from September through November 2025 represented one of the most critical vulnerability windows in recent cybersecurity history. Security research teams identified over 1,200 high-risk vulnerabilities, with 58 actively exploited in real-world attacks. Three vulnerabilities achieved the maximum CVSS 10.0 score (indicating complete system compromise via network without authentication), marking this period as exceptionally severe for enterprise defenders. The threat landscape was dominated by remote code execution (RCE) flaws (45-60% of major vulnerabilities) and privilege escalation attacks targeting Microsoft, Cisco, Oracle, and Fortinet infrastructure

CVE ID	Month	Product	Vuln type	CVSS	Exploit	Impact
CVE-2025-20337	Nov	Cisco ISE	Unauth RCE	10	Active	Critical
CVE-2025-42890	Nov	SAP SQL Mon	Creds RCE	10	HighRisk	Critical
CVE-2025-61882	Oct	Oracle E-Biz	Unauth RCE	10	Active	Critical
CVE-2025-49708	Oct	MS Graphics	UAF EoP	9.9	HighRisk	Critical
CVE-2025-54253	Oct	Adobe AEM	OGNL RCE	9.8	Active	Critical
CVE-2025-59230	Oct	Windows Ras	PrivEsc	9.8	Active	Critical
CVE-2025-59246	Oct	Entra ID	PrivEsc	9.8	HighRisk	Critical
CVE-2025-59287	Oct	MS WSUS	Deserial RCE	9.8	Active	Critical
CVE-2025-64446	Oct	FortiWeb	PathTrav RCE	9.8	Active	Critical
CVE-2025-53690	Sep	Sitecore XM	ViewState Deser	9.5	Active	Critical
CVE-2025-10035	Sep	GoAnywhere	Deserial RCE	9	Active	Critical
CVE-2025-5777	Nov	NetScaler	Mem leak	9	Active	Critical
CVE-2025-20333	Sep	Cisco ASA	BuffOvf RCE	8.8	Active	Critical
CVE-2025-59236	Oct	MS Excel	UAF RCE	8.4	Active	High
CVE-2025-59291	Oct	Azure CCI	Cont escape	8.2	HighRisk	Critical

1. Vulnerability Landscape Overview

1.1 September 2025 – Foundation of the Campaigns

Recorded Future's Insikt Group identified 1,096 vulnerabilities with severity scores of 65 or above during September, with 16 rated as actively exploited. The month was dominated by buffer overflow and deserialization flaws affecting networking appliances and content management systems. The vulnerability targeting Cisco Adaptive Security Appliance (ASA) devices—specifically CVE-2025-20333 and CVE-2025-20362 chained together—represented a watershed moment: attackers deployed a sophisticated bootkit called RayInitiator to gain persistent control over VPN infrastructure. Meanwhile, Sitecore Experience Manager (CVE-2025-53690) deployments using legacy machine keys from 2017 guidance fell victim to attackers delivering tools like WEEPSTEEL (reconnaissance), EARTHWORM (tunneling), and SharpHound (Active Directory enumeration)

Reference - https://www.recordedfuture.com/blog/september-2025-cve-landscape

1.2 October 2025 – Peak Vulnerability Activity

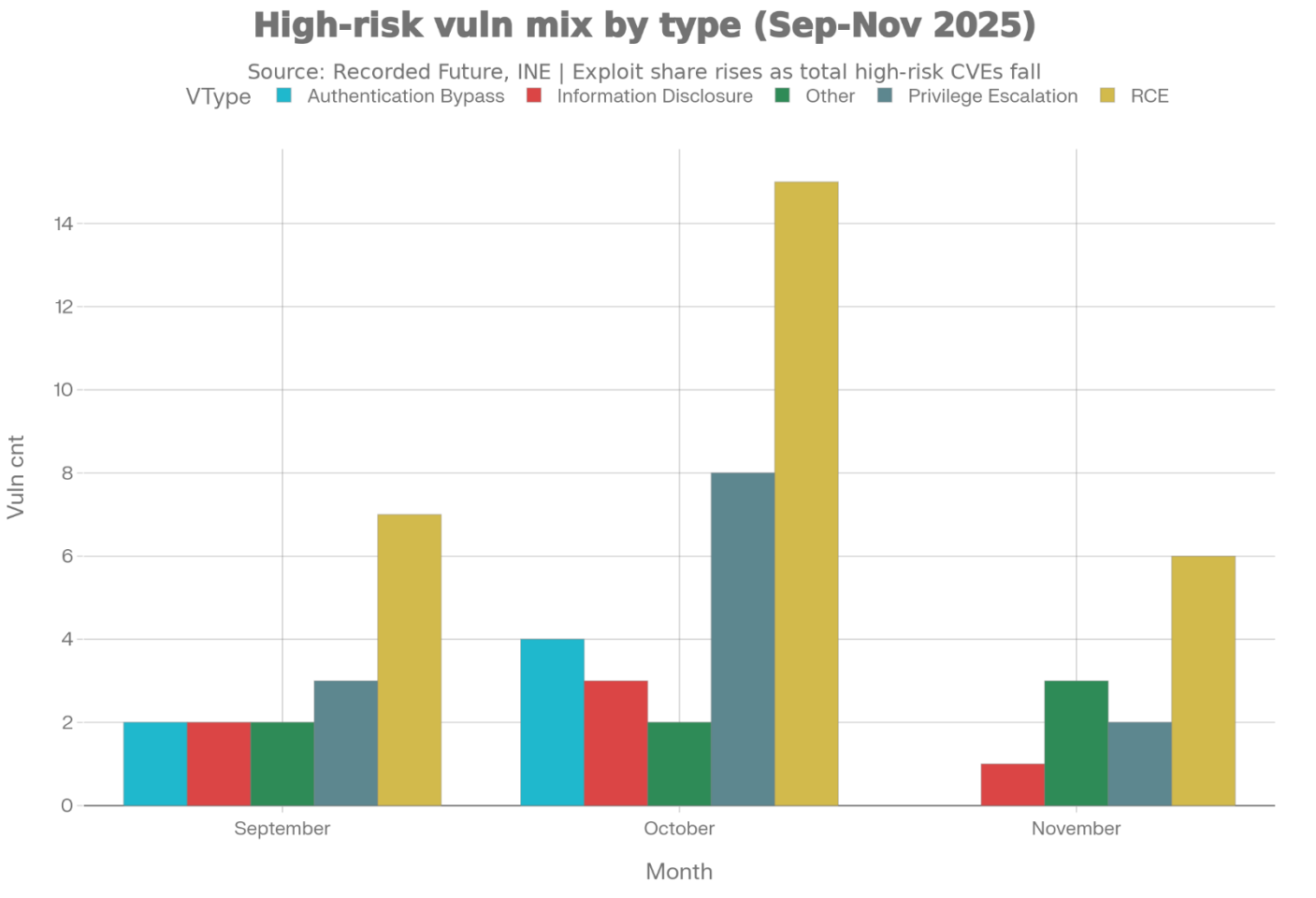
October delivered unprecedented scale: Microsoft released 175 security patches in a single Patch Tuesday cycle—the largest monthly release on record. Recorded Future's Insikt Group identified 32 high-impact vulnerabilities, with 26 achieving "Very Critical" risk scores. The month was defined by two dominant threat campaigns: CL0P ransomware group's exploitation of Oracle E-Business Suite zero-day (CVE-2025-61882) for data theft and extortion, and threat actors targeting Microsoft WSUS deserialization flaw (CVE-2025-59287) to compromise update infrastructure. Enterprise defenders faced cascading risks—vulnerabilities across Microsoft, Oracle, Adobe, Fortinet, Azure, and Citrix required simultaneous mitigation. The Common Weakness Enumeration (CWE) analysis revealed that improper authentication (CWE-287) was the dominant flaw pattern, followed by out-of-bounds writes and path traversal vulnerabilities.

Reference - https://www.recordedfuture.com/blog/october-2025-cve-landscape

1.3 November 2025 – Fewer Bugs, Higher Severity

November delivered the month's most severe individual vulnerabilities. Cisco ISE (Identity Services Engine)—a core authentication and network access control system deployed across enterprises—fell victim to unauthenticated RCE (CVE-2025-20337, CVSS 10.0). SAP SQL Anywhere Monitor and Cisco ISE joined an unprecedented cohort of three CVSS 10.0 vulnerabilities affecting web-based systems. Google Chrome's V8 JavaScript engine disclosed its seventh actively exploited zero-day of the year (CVE-2025-13223), prompting emergency browser updates. Microsoft Office Preview Pane (CVE-2025-62199) and Visual Studio (CVE-2025-62214) received RCE patches, demonstrating supply-chain risk vectors targeting developers and knowledge workers

Reference - https://ine.com/blog/november-2025-critical-cve-round-up



2. Top 15 Critical Web-Exposed CVEs (Sep–Nov 2025)

2.1 CVE-2025-20337 – Cisco Identity Services Engine (ISE) Unauthenticated RCE

Aspect	Details
Product	Cisco ISE (all versions)
Vulnerability Type	Authentication Bypass + Remote Code Execution
CVSS Score	10.0 (Maximum)
Exploitation Status	Actively exploited; web shells observed
Impact	Complete root-level access to network identity infrastructure
Detection Evidence	"IdentityAuditAction" web shell indicators
Remediation Timeframe	Immediate (within 24 hours for exposed systems)

Cisco ISE is the identity and network access control backbone for enterprise authentication flows. CVE-2025-20337 enables attackers to bypass all authentication mechanisms and execute arbitrary code with root privileges. Cloud security teams detected active exploitation delivering custom web shells for persistent access. The vulnerability is particularly dangerous because ISE systems often sit between users and critical infrastructure, providing attackers a central control point for lateral movement. Post-exploitation investigations must focus on Tomcat web application logs, unauthorized administrator account creation, and unknown Java Archive (JAR) file deployments in the ISE application directory

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-20337

Git hub - https://github.com/Ashwesker/Blackash-CVE-2025-20337

You tube - https://youtu.be/LUKgRuOrwxU?si=nlrVoMKf4dK_PfSx

2.2 CVE-2025-61882 – Oracle E-Business Suite Unauthenticated RCE (CLoP Campaign)

Aspect	Details
Product	Oracle EBS 12.2.3 through 12.2.14
Vulnerability Type	Chained: SSRF → CRLF Injection → XSL Template Injection
CVSS Score	10.0 (Zero-day)

Aspect	Details
Exploitation Status	Actively exploited by CL0P ransomware group
Threat Actors	CL0P (multi-stage Java infection: GOLDVEIN.JAVA → SAGEGIFT → SAGELEAF → SAGEWAVE)
Exposed Instances	~1,430 on Shodan (US, China, Germany, India, UK)
Attribution Evidence	Extortion emails from addresses active on CL0P's leak site since May 2025

CVE-2025-61882 is a complex attack that shows how modern supply-chain exploits work, but it can be explained more simply. Attackers send a malicious XML request to a vulnerable servlet, which allows them to force the server to make internal requests (SSRF). They then abuse HTTP header manipulation and path traversal to access internal JSP pages. By injecting a malicious XSL stylesheet, they can execute code on the server, leading to full remote code execution (RCE). After gaining access, attackers run basic system and network commands to understand the environment and install a servlet-based backdoor to maintain access and steal credentials.

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-61882

Oracle - https://www.oracle.com/security-alerts/alert-cve-2025-61882.html

Git hub - https://github.com/watchtowrlabs/watchTowr-vs-Oracle-E-Business-Suite-CVE-2025-61882

You tube - https://youtu.be/kxXSQWojYTI?si=4FNXCAG7omFgU7uB

2.3 CVE-2025-42890 – SAP SQL Anywhere Monitor Hardcoded Credentials RCE

Aspect	Details
Product	SAP SQL Anywhere Monitor (Non-GUI)
Vulnerability Type	Hardcoded Credentials + Authentication Bypass
CVSS Score	10.0
Severity Classification	SAP HotNews (highest priority)
Root Cause	Default credentials embedded in application binary
Patch Reference	SAP Note 3666261; Requires SQL Anywhere 17.0 SP1 PL20+
Enterprise Impact	Affects embedded SQL Anywhere monitoring deployments

CVE-2025-42890 is a credential-related vulnerability that highlights the danger of hardcoded authentication in monitoring systems. This flaw allows attackers to gain full remote access without proper authentication, letting them change database settings, steal credentials from monitoring logs, and move deeper into backend database systems. Its highest-priority rating shows how critical it is to secure database monitoring tools, especially in sensitive sectors like healthcare, finance, and government

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-42890

SAP - https://support.sap.com/en/my-support/knowledge-base/security-notes-news/november-2025.html

Tenable - https://www.tenable.com/cve/CVE-2025-42890

2.4 CVE-2025-49708 – Microsoft Graphics Component Use-After-Free (Privilege Escalation)

Aspect	Details
Vulnerability Type	Use-After-Free (Memory Corruption) → SYSTEM Escalation
CVSS Score	9.9
Affected Versions	Windows 10, 11, Server 2012-2025
Attack Vector	Locally crafted graphics payload or malicious document
Exploitation Likelihood	High (exploitable via Office documents, PDF rendering)
Risk to Hypervisors	Guest-to-host escape potential in virtualized environments

This vulnerability affects the Windows GDI+ graphics library, a core system component used to display images across the operating system. By using specially crafted image data, an attacker can trigger a memory error where freed memory is reused, allowing them to control system memory. Because GDI+ is used by common applications like Word, Excel, PDF readers, and web browsers, the risk is widespread—malicious images embedded in documents can exploit the flaw. Successful attacks can allow a low-privileged user to gain full SYSTEM access, and in virtualized environments, this could even lead to escaping from a virtual machine to the host system

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-49708

Tenable - https://www.tenable.com/cve/CVE-2025-49708

Microsoft - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49708

You tube - https://youtu.be/EvIHAhjrBVQ?si=7AEsySKWIMKuOAPQ

2.5 CVE-2025-59287 – Microsoft WSUS Deserialization RCE

Aspect	Details
Vulnerability Type	Unsafe Deserialization of AuthorizationCookie
CVSS Score	9.8
Exploitation Status	Actively exploited; public PoC released
Attack Path	Unauthenticated HTTP POST to WSUS web service
Patch Status	Microsoft out-of-band update released October 23, 2025
Exposed Systems	~25 publicly exposed WSUS instances
Industry Impact	Affects centralized patch distribution infrastructure

CVE-2025-59287 is a critical vulnerability in Windows Server Update Services (WSUS) that targets enterprise patch management systems. WSUS improperly processes untrusted authentication cookie data, allowing attackers to execute code with SYSTEM-level privileges. Since WSUS has high privileges and controls patch distribution, attackers can abuse this access to push malicious updates to many systems or disrupt legitimate updates, creating a serious supply-chain risk. The flaw has been actively exploited on internet-exposed WSUS servers, where attackers used built-in tools to steal data and run commands under the WSUS service

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-59287

Tenable https://github.com/jiansiting/CVE-2025-59287

Microsoft - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287?ref=thestack.technology

You tube - https://youtu.be/GKp9hnysMOE?si=qXMBROCir3LFqhKE

2.6 CVE-2025-59246 – Azure Entra ID (Azure AD) Privilege Escalation

Aspect	Details
Vulnerability Type	Authorization Logic Flaw in Identity Workflows
CVSS Score	9.8
Impact Scope	Cloud tenant-level privilege escalation to Global Administrator
Attack Method	Chained API calls exploiting insufficient authorization checks
Post-Exploitation Risks	Unauthorized role assignment, MFA enrollment changes, app consent abuse

Aspect	Details
Remediation	Convert permanent admin roles to Privileged Identity Management (PIM)

This vulnerability in Azure Entra ID shows how cloud identity platforms can be abused for privilege escalation. Weak authorization checks allow low-privileged users to make API calls that should be restricted to administrators. By chaining these calls, attackers can assign themselves high-level roles, disable security controls like MFA, and grant application permissions that enable account takeover through OAuth. The attack is especially dangerous because it is fully API-based and happens entirely inside the tenant, without needing any external network access.

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-59246

Tenable https://www.tenable.com/cve/CVE-2025-59246

Microsoft - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59246

2.7 CVE-2025-59230 – Windows RasMan Privilege Escalation

Aspect	Details
Vulnerability Type	Insufficient Access Validation → SYSTEM Escalation
CVSS Score	9.8
Affected Versions	Windows 10 1607-22H2; Server 2008-2025
Exploitation Status	Actively exploited in post-compromise scenarios
Attack Chain	Initial access (phishing/RDP) → CVE-2025-59230 → SYSTEM → Lateral Movement
Mitigation	Disable RasMan if not required; enforce LAPS and MFA

RasMan (Remote Access Connection Manager) is a Windows service responsible for managing dial-up and VPN connections. This vulnerability occurs because RasMan does not properly validate access to certain privileged functions, allowing local attackers to escalate their privileges. After gaining an initial foothold through methods like phishing, stolen credentials, or insecure RDP access, attackers can exploit CVE-2025-59230 to obtain SYSTEM-level control. This level of access allows them to maintain persistence, harvest credentials, and move laterally across the network.

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-59230

You tube - https://youtu.be/TBPlOXhgX14?si=z7dKVbGnunfJhRFv

Microsoft - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59230

2.8 CVE-2025-64446 – Fortinet FortiWeb Path Traversal RCE

Aspect	Details
Product	FortiWeb Web Application Firewall
Vulnerability Type	Unauthenticated Path Traversal + Admin Account Creation
CVSS Score	9.8
Exploitation Status	Actively exploited since early October 2025
CISA KEV Status	Added to Known Exploited Vulnerabilities catalog
Attack Pattern	Crafted HTTP POST requests create unauthorized admin accounts
Patch Version	FortiWeb 8.0.2+
Real-World Impact	Internet-facing WAF appliances in scope for mass scanning

FortiWeb is a commonly used Web Application Firewall that protects public-facing web applications. CVE-2025-64446 allows attackers to bypass authentication by abusing a path traversal flaw in HTTP requests, enabling them to create their own administrator accounts. With admin access, attackers can weaken security rules, turn off logging, redirect traffic to malicious servers, or intercept encrypted HTTPS traffic. The flaw impacted thousands of FortiWeb systems worldwide and was quickly targeted by large-scale scanning and exploitation campaigns after it became public

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-64446

You tube - https://youtu.be/fNHdKaRBDas?si=qrWs-VwFc8LmwleV

You tube - https://youtu.be/zLL2d8zprDU?si=Ume2tagImD--AnYT

Forti guard - https://fortiguard.fortinet.com/psirt/FG-IR-25-910

2.9 CVE-2025-54253 – Adobe AEM Forms OGNL RCE

Aspect	Details
Vulnerability Type	Authentication Bypass + OGNL Expression Language Injection
CVSS Score	9.8
Root Cause	DevMode enabled in Struts2 framework; SecurityFilter bypass via "login." in URL
Exploitation Method	`GET /adminui/updateLicense1.do;login.?debug=command&expression=7*7`
Proof of Concept	Publicly available; weaponization confirmed in active campaigns

Aspect	Details
Exposed Instances	~418 AEM instances on Shodan (US, Australia, Germany, Canada, Ireland)
Remediation	Upgrade to AEM 6.5.0-0108+

CVE-2025-54253 affects Adobe Experience Manager systems running with DevMode enabled. An authentication bypass allows certain login-related URLs to slip past security checks, and when combined with OGNL expression injection in Struts2 DevMode, attackers can execute arbitrary Java code. Because AEM often hosts public-facing customer websites, successful exploitation can let attackers alter site content, inject malware, or steal sensitive customer data from the CMS database

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-54253

You tube - https://youtu.be/JE53nIhRH_c?si=HAiuVsD1sf1aKe9q

Adobe - https://helpx.adobe.com/in/security/products/aem-forms/apsb25-82.html

Git hub - https://github.com/Ashwesker/Blackash-CVE-2025-54253

2.10 CVE-2025-53690 – Sitecore ViewState Deserialization RCE

Aspect	Details
Product	Sitecore XM, XP, XC (versions 9.0 and earlier)
Vulnerability Type	Unsafe ViewState Deserialization via Exposed Machine Key
CVSS Score	9.5 (estimated from Very Critical classification)
Root Cause	Sample ASP.NET machine keys published in 2017 deployment guides
Exploitation Method	POST to `/sitecore/blocked.aspx` with forged ViewState using known machine key
Post-Exploitation	Deploy .NET assemblies (WEEPSTEEL for reconnaissance, EARTHWORM for tunneling)
Detection	ASP.NET Application log Event ID 1316 (ViewState verification failed)
Exposed Instances	~330 Sitecore instances on Shodan

CVE-2025-53690 shows how insecure configuration defaults can turn into long-term security risks. Sitecore documentation included sample ASP.NET machine keys meant for testing, but many organizations mistakenly used them in production. Attackers could exploit these static keys to create malicious ViewState data and run harmful code on the server. Real-world attacks used tools to gather system and network information, tunnel traffic to command-and-control servers, and map Active Directory. This case highlights how failing to change default or example configurations can leave systems exposed for years.

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-53690

You tube - https://youtu.be/htqzwIyjotw?si=nGItEOGsoZKgXx8b

Tenable - https://www.tenable.com/cve/CVE-2025-53690

Git hub - https://github.com/rxerium/CVE-2025-53690

2.11 CVE-2025-5777 – Citrix NetScaler "CitrixBleed 2" Memory Leak

Aspect	Details
Vulnerability Type	Memory Over-Read → Session/Credential Theft
CVSS Score	9.0
Product	Citrix Gateway and ADC (Application Delivery Controller)
Exploitation Status	Actively exploited in multi-vector breach campaigns
Attack Pattern	Extract administrator session cookies and VPN credentials
Remediation	Patch per Citrix advisory; invalidate active sessions; rotate credentials
Industry Context	Continuation of "CitrixBleed" vulnerabilities affecting VPN infrastructure

CVE-2025-5777 is a follow-up to the original CitrixBleed issue and highlights ongoing memory safety problems in Citrix systems. The vulnerability allows attackers to read sensitive data from memory, including active session tokens and VPN credentials. Since Citrix Gateways control remote access for employees, stealing these credentials can give attackers administrator-level access, allowing them to change security settings, monitor user traffic, or install backdoors that impact large numbers of remote users.

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-5777

You tube - https://www.youtube.com/watch?v=A9cp4I-9ifs

Arctic Wolf: https://arcticwolf.com/resources/blog/cve-2025-5777/

Git hub - https://github.com/RickGeex/CVE-2025-5777-CitrixBleed

---

2.12 CVE-2025-59236 – Microsoft Excel Use-After-Free RCE

Aspect	Details
Vulnerability Type	Use-After-Free (Memory Corruption) in Object Parsing
CVSS Score	8.4

Aspect	Details
Attack Vector	Malicious .xlsx file via email attachment or web download
Exploitation Status	Weaponized in opportunistic phishing campaigns
Exploitation Complexity	Low—no macros or user code execution required; triggered by file open
Remediation	Apply Microsoft Office security updates; disable Preview Pane in email

CVE-2025-59236 is a vulnerability in Microsoft Excel related to how it processes certain objects inside spreadsheet files. Specially crafted `.xlsx` files can trigger a memory error that allows attackers to run malicious code with the same privileges as the user. This is especially dangerous because Excel files are commonly shared in organizations, and the attack does not rely on macros. Simply opening the file—or even previewing it in an email client—can be enough to trigger the exploit

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-59236

Microsoft - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59236

Wiz - https://www.wiz.io/vulnerability-database/cve/cve-2025-59236

Akaoma: https://cve.akaoma.com/cve-2025-59236

2.13 CVE-2025-20333 & CVE-2025-20362 – Cisco ASA Chained RCE/Auth Bypass (RayInitiator Campaign)

Aspect	Details
Products	Cisco ASA 5500-X series (firmware versions 9.12.4.67, 9.14.4.24 without Secure Boot)
Vulnerability Types	Buffer Overflow + Missing Authorization
CVSS Combined Impact	Enables unauthenticated complete ASA compromise
Post-Exploitation Malware	RayInitiator (bootkit) + LINE VIPER (modular shellcode)
Attribution	Evolution of ArcaneDoor campaign (April 2024)
Persistence Mechanism	GRUB/ROMMON modification enabling pre-OS boot interception
Threat Operations	Continued targeting of VPN infrastructure for remote access control

CVE-2025-20333 and CVE-2025-20362 are chained flaws affecting **Cisco ASA** VPN systems. A buffer overflow in web services, combined with a missing authorization check, allows attackers to fully compromise vulnerable VPN gateways. According to investigations by **CISA** and **NCSC**, attackers used this access to deploy *RayInitiator*, a stealthy boot-level backdoor that runs before the operating system and survives reboots and updates. This gives attackers long-term control, letting them steal VPN credentials, monitor user sessions, and extract data passing through the VPN.

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-20333

Cisco - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB

Tenable: https://www.tenable.com/blog/cve-2025-20333-cve-2025-20362-faq-cisco-asa-ftd-zero-days-uat4356

YouTube: https://www.youtube.com/watch?v=4-7Q1tFweF0

2.14 CVE-2025-10035 – Fortra GoAnywhere MFT Deserialization RCE

Aspect	Details
Vulnerability Type	Unsafe Deserialization in License Servlet
CVSS Score	9.0
Threat Actor	Storm-1175 cybercriminal group
Post-Exploitation Payload	Medusa ransomware + SimpleHelp/MeshAgent remote monitoring tools
Active Exploitation	Ongoing since September 11, 2025
Industry Impact	GoAnywhere is widely used for secure file transfer in enterprises

CVE-2025-10035 affects **GoAnywhere**, a tool used for secure business file transfers. The vulnerability is caused by unsafe Java deserialization in a license-checking component, which allows remote attackers to run arbitrary code on the server. The threat group **Storm-1175** exploited this flaw to deploy **Medusa ransomware**, using legitimate remote access tools to maintain persistence. This enabled attackers to encrypt files and carry out ransomware extortion campaigns against affected organizations

Resources to Learn More

Nist - https://nvd.nist.gov/vuln/detail/CVE-2025-10035

Microsoft - https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed

Exploitation Blog - https://labs.watchtowr.com/it-is-bad-exploitation-of-fortra-goanywhere-mft-cve-2025-10035-part-2

2.15 CVE-2025-59291 – Azure Confidential Container Instances Container Escape

Aspect	Details
Vulnerability Type	Improper Path Validation in Resource Mounting
CVSS Score	8.2
Impact Scope	Privilege escalation + container isolation breach
Attack Method	Symbolic link manipulation during resource mount operations
Affected Workloads	Confidential computing environments protecting encrypted data
Remediation Complexity	Requires container image rebuilding and redeployment

CVE-2025-59291 affects **Azure Confidential Container Instances**, a service designed to securely run sensitive workloads. The vulnerability allows attackers to escape container isolation by abusing a path traversal flaw during resource mounting. By creating malicious symbolic links, attackers can access protected host files, including encryption keys, data from other containers, or system-level secrets. This issue is especially serious for regulated sectors like healthcare and finance, where confidential computing is relied on to meet strict security and compliance requirements.

Resources to Learn More

NIST: https://nvd.nist.gov/vuln/detail/CVE-2025-59291

Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59291

Strobes: https://strobes.co/blog/top-cves-of-october-2025

Akaoma: https://cve.akaoma.com/cve-2025-59291

Conclusion

The September-November 2025 period represents a defining vulnerability cycle: three CVEs achieved perfect exploitation scores (10.0), threat actors weaponized zero-days within hours of disclosure, and enterprise defenders faced cascading patching challenges across multiple vendor ecosystems. For cybersecurity professionals pursuing CEH certification and practical security research, this period demonstrates that vulnerability analysis extends far beyond severity scores—context (exploitation activity, threat actor attribution, supply-chain implications) and remediation complexity determine real-world risk.