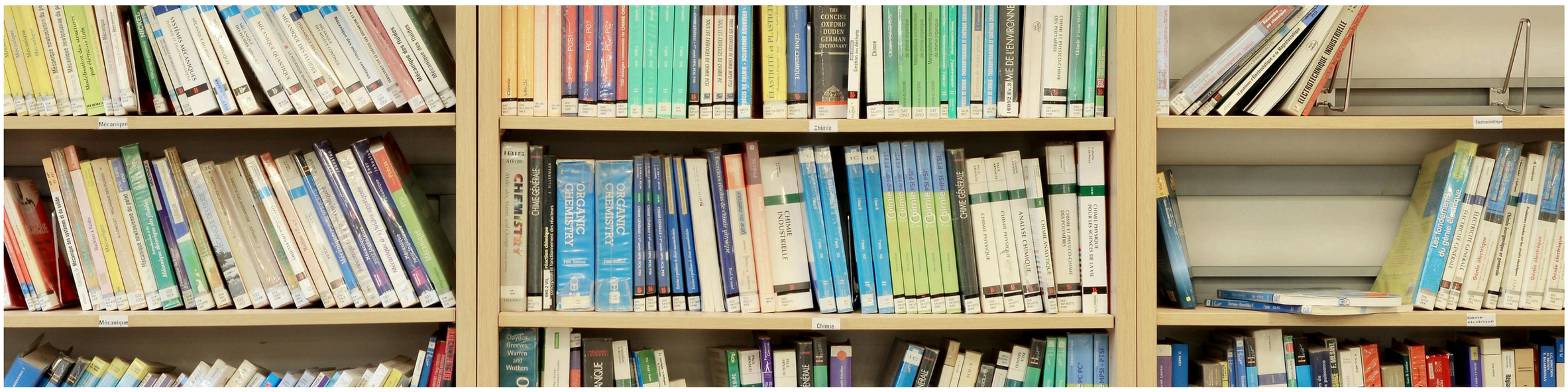
Knowledge Alert

JHSConsulting

January 29, 2026



CERT-In VULNERABILITY INTELLIGENCE BRIEF

10-Month Analysis: April 2025 - January 2026 | With Vulnerability Type Analysis & Remediation Guide

281 TOTAL	55 CRITICAL	197 HIGH	25 MEDIUM	4 ADVISORIES

10-MONTH VULNERABILITY TREND

Apr 2025	▬▬▬▬▬▬▬▬	17
May 2025	▬▬▬▬▬▬▬▬	16
Jun 2025	▬▬▬▬▬▬▬▬▬▬	22
Jul 2025	▬▬▬▬▬▬▬▬▬	20
Aug 2025	▬▬▬▬▬▬▬▬▬▬▬▬	28
Sep 2025	▬▬▬▬▬▬▬▬▬▬▬▬	27
Oct 2025	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬	44
Nov 2025	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬	46
Dec 2025	▬▬▬▬▬▬▬▬▬▬▬▬▬	31
Jan 2026	▬▬▬▬▬▬▬▬▬▬▬	26

Peak: Nov 2025 (46) | 171% surge from Apr to Nov | Stabilizing in Jan 2026

VENDOR RISK MATRIX

Vendor	Total	Critical	Trend	Priority	SLA
Cisco	38	**6**	↑	**URGENT**	**48h**
Microsoft	28	**8**	↑	**URGENT**	**48h**
Google (Chrome/Android)	32	**5**	→	**URGENT**	**48h**
Fortinet	14	**5**	↑	**URGENT**	**48h**
Mozilla	14	0	→	**PRIORITY**	**7d**
GitLab	15	**1**	→	**PRIORITY**	**7d**

Vendor	Total	Critical	Trend	Priority	SLA
HPE/Aruba	12	0	↑	**PRIORITY**	**7d**
Oracle	12	**4**	→	**URGENT**	**48h**
Apache	10	**1**	→	**PRIORITY**	**7d**
VMware	8	0	↓	**ROUTINE**	**30d**

Vulnerability Type-Wise Analysis

Comprehensive breakdown of 281 vulnerabilities by attack type, affected products, and business impact

Vulnerability Type	Count	Share	Trend	Key Affected Products	Business Impact
Remote Code Execution (RCE) CRITICAL	**58**	**21%**	↑	Microsoft Office/Windows, Google Chrome, Cisco IOS, Fortinet, Oracle, n8n	Complete system takeover, data theft, ransomware deployment, lateral movement
Multiple Vulnerabilities (Bundled) HIGH	**98**	**35%**	↑	All major vendors - typically monthly/quarterly security updates	Varies by component - cumulative risk is significant
Privilege Escalation HIGH	**28**	**10%**	↑	Windows Kernel, Cisco ISE, Grafana, SolarWinds, Splunk, Linux	Admin/root access, security control bypass, persistent access
Authentication Bypass CRITICAL	**22**	**8%**	↑↑	Linksys, ASUS routers, CrushFTP, WordPress plugins, Cisco TACACS+	Unauthorized access, account takeover, identity theft, data breach
Denial of Service (DoS) HIGH	**24**	**9%**	→	Cisco, F5 BIG-IP, Palo Alto, Apache Tomcat, ISC Bind, Vercel Next.js	Service disruption, availability loss, business continuity impact
Cross-Site Scripting (XSS) MEDIUM	**18**	**6%**	→	Cisco products, Grafana, Zimbra, Drupal, WordPress, Junos Space	Session hijacking, credential theft, defacement, phishing
Information Disclosure MEDIUM	**12**	**4%**	→	Cisco, Oracle E-Business, MongoDB, Desktop Window Manager, Linux	Sensitive data exposure, reconnaissance for further attacks
SQL/Command Injection CRITICAL	**10**	**4%**	↑	FortiWeb, Cisco REST API, Fortra GoAnywhere MFT, Kibana	Database compromise, command execution, data manipulation
Security Feature Bypass HIGH	**8**	**3%**	↑	Windows Secure Boot, Cisco Secure Boot, WhatsApp, Chrome	Security control circumvention, protection mechanism failure
Path Traversal / File Access HIGH	**5**	**2%**	→	Fortinet FortiWeb, WordPress plugins, various web applications	Arbitrary file read/write, configuration exposure, code execution
Buffer Overflow / Memory Corruption CRITICAL	**6**	**2%**	→	Net-SNMP, Dahua products, Apple products, Chrome V8	Code execution, system crash, memory disclosure
XML External Entity (XXE) HIGH	**4**	**1%**	→	SysAid On-Prem, Apache Tika, various XML parsers	Server-side request forgery, file disclosure, DoS
Cross-Site Request Forgery (CSRF) MEDIUM	**4**	**1%**	↓	Drupal modules, various web applications	Unauthorized actions on behalf of users

VULNERABILITY TYPE: ATTACK VECTORS & MITIGATIONS

Vulnerability Type	Attack Vector & Exploitability	Recommended Mitigations
Remote Code Execution	Network-based, often no auth required Exploitability: HIGH - Active exploits exist	Priority patching within 48hrs; Network segmentation; IDS/IPS signatures; Disable unnecessary services
Multiple Vulnerabilities	Various attack vectors combined Exploitability: MEDIUM - Assess individual CVEs	Regular patch cycles; Vulnerability scanning; Risk-based prioritization; Change management
Privilege Escalation	Local or authenticated access required Exploitability: MEDIUM - Often chained	Principle of least privilege; PAM solutions; Monitor admin activities; Regular access reviews
Authentication Bypass	Network-based, no credentials needed Exploitability: HIGH - Trivial to exploit	Enable MFA everywhere; Update firmware immediately; Network access controls; Zero trust architecture
Denial of Service	Network-based, unauthenticated Exploitability: HIGH - Easy to execute	DDoS protection; Rate limiting; Redundancy/failover; Traffic analysis and filtering
Cross-Site Scripting	Requires user interaction Exploitability: MEDIUM - Social engineering	Input validation; Content Security Policy; HTTPOnly cookies; Security awareness training
SQL/Command Injection	Network-based via malicious input Exploitability: HIGH - Well-known techniques	Parameterized queries; Input validation; WAF deployment; Code review and SAST
Security Feature Bypass	Varies by vulnerability Exploitability: MEDIUM - Specific conditions	Defense in depth; Multiple security layers; Configuration hardening; Regular audits

KEY VULNERABILITIES: IMPACT & REMEDIATION GUIDE

Category	Key Vulnerabilities	Risk Impact	Remediation Actions
Microsoft Windows & Office (28 vulns)	RCE in LSASS, Word, Excel, Windows Graphics; Privilege escalation	Complete system compromise, ransomware	January 2026 Patch Tuesday; Enable Credential Guard
Google Chrome & Android (32 vulns)	RCE, use-after-free, heap buffer overflow in V8 engine	Browser compromise, mobile takeover	Enable auto-update; MDM patches; Block old browsers
Cisco Network Equipment (38 vulns)	Command injection, TACACS+ auth bypass, SNMP RCE	Network infrastructure compromise	Update IOS/IOS XE; Restrict SNMP; Segment management
Fortinet Security Products (14 vulns)	RCE in FortiSIEM, SQL injection in FortiWeb, path traversal	Perimeter breach, data exfiltration	Priority patching; Review firewall rules; MFA for admin
Oracle & SAP Enterprise (12 vulns)	Critical patches for Oracle DB, E-Business Suite, Identity Manager	Business app compromise, financial exposure	Schedule maintenance windows; Test before deploy
Authentication Systems (22 vulns)	Auth bypass in routers, apps, plugins, enterprise systems	Unauthorized access, identity theft	Enable MFA everywhere; Update firmware; Audit auth

🔍 KEY TRENDS & STRATEGIC INSIGHTS

1. RCE Dominance (21%): Remote Code Execution remains top threat - prioritize network segmentation and patch management.
2. Auth Bypass Surge (↑↑): 22 authentication bypass vulnerabilities - MFA implementation now critical across all systems.
3. Perimeter Under Attack: 52+ vulnerabilities in Cisco/Fortinet/HPE - network boundary security needs immediate attention.
4. Injection Attacks Persistent: SQL/Command injection still prevalent - input validation and WAF deployment essential.
5. Browser Security Fatigue: 32 Chrome/Edge vulnerabilities - automate browser updates, consider browser isolation.

✅ ACTION PRIORITY MATRIX

Timeline	Target Systems	Actions
0-48 HRS	Microsoft, Fortinet, Cisco, Oracle - all RCE vulnerabilities	Emergency patching; Network isolation; Enable monitoring
1-7 DAYS	Browsers, Android, HPE/Aruba, Auth bypass vulns	Verify auto-updates; MDM patches; Enable MFA; Firmware updates
7-30 DAYS	VMware, GitLab, SAP, Apache, XSS/CSRF vulns	Scheduled maintenance; Staging tests; WAF rules; CSP headers

🤝 JHS CYBERSECURITY SERVICES (CERT-IN EMPANELLED)

VAPT Services Network, Application, Cloud, API testing	**Compliance Audits** RBI, SEBI, IRDAI, DPDP Act, ISO 27001
Security Assessment Infrastructure review, patch management audit	**Incident Response** Forensics, investigation, remediation support

KNOWLEDGE DESK

~***Abutalib Syed***
(Knowledge Executive)

~ Taher Pepermintwala
(FCA, CISA)

T: +91 80970 95056

E: CONNECT@JHSCONSULTING.IN