DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DoD CYBER CRIME CENTER (DC3)

DIB-REPORTED CYBER THREATS: CY 2026 | Q2 (APR – JUN)

DC3 DCISE receives voluntary reporting from Defense Industrial Base (DIB) companies through the DoW's DIB Cybersecurity (CS) Program and mandatory reporting as required by DFARS clause 252.204-7012. This product describes trends in cyber activity reported to DC3 DCISE, as well as noteworthy cyber events occurring in CY26 Q2.

DIB REPORTING AT A GLANCE

64% Improper Handling/ Misconfiguration Indents

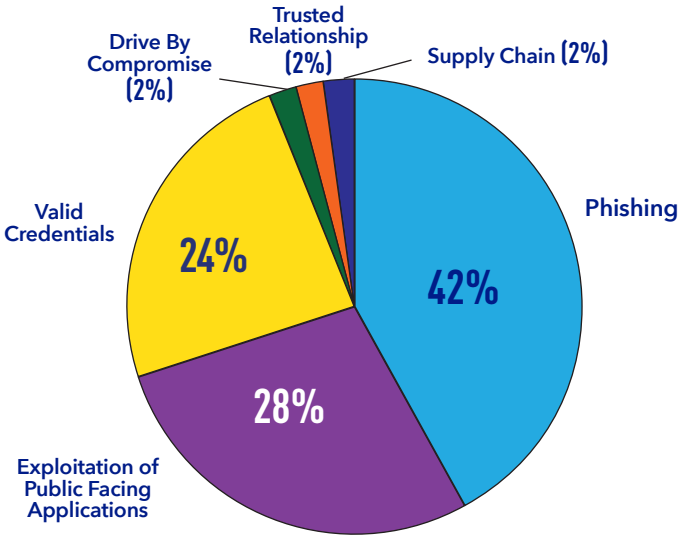
36% Unauthorized Access Incidents

41% Ransomware Incidents

48% Unattributed Incidents

11% Suspected State-Sponsored Incidents

IDENTIFIED INITIAL ACCESS VECTORS

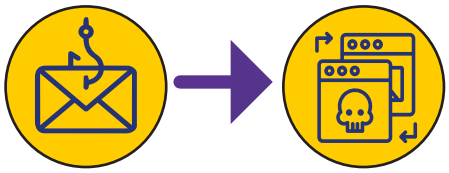


TOP THREE REPORTED RANSOMWARE VARIANTS

1. INC RANSOMWARE
2. AKIRA
3. DRAGONFORCE

TECHNIQUE OF THE QUARTER

Attackers may use phishing techniques to exploit OAuth's by-design redirection mechanism. Victims can be redirected to attacker-controlled infrastructure hosting malware, allowing the attacker to maintain persistence.



Interested in joining the DIB CS Program? Contact us at DC3.DIB.CSRegistration@us.af.mil.

DCISE, a directorate within the DoD Cyber Crime Center, is the operational hub of the DoW's DIB Cybersecurity Program. DCISE develops and shares actionable threat products, performs cyber analysis and diagnostics, and provides remediation consultation for DIB participants.

@DC3DCISE DC3.DCISE@us.af.mil 887.838.2174 | 410.981.0104

DoD—Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DoD CYBER CRIME CENTER (DC3)

DIB-REPORTED CYBER THREATS: CY 2026 | Q2 (APR – JUN)

IVANTI ENDPOINT MANAGER EXPLOITATION

Narrative: On 7 May 26, Ivanti published a security advisory addressing CVE-2026-6973 (CVSS v3 score 7.2) in Endpoint Manager Mobile (EPMM). The vulnerability stems from improper input validation and allows a remotely authenticated user with administrative access to achieve remote code execution (RCE). According to Ivanti, active zero-day exploitation affected a limited number of users.

Suspected Threat Actor: Unknown actors

CVE(s): CVE-2026-6973 (RCE)

TTP(s): Exploit Public-Facing Application [T1190]

DCISE Reporting: Alert 26-016

Open-Source Reporting: https://www.ivanti.com/blog/may-2026-epmm-security-update

FORTICLIENT EMS EXPLOITED

Narrative: On 4 Apr 26, Fortinet released a security advisory detailing a zero-day vulnerability, tracked as CVE2026-35616 (CVSS v3 score 9.1), affecting FortiClient Enterprise Management Server (EMS). This unauthenticated API bypass allowed threat actors to abuse the EMS policy deployment mechanism to deliver "EKZ", a newly discovered credential stealer targeting Chrome and Firefox.

Suspected Threat Actor: Unknown

CVE(s): CVE-2026-35616 (Authentication Bypass)

TTP(s): Exploit Public-Facing Application [T1190], Credentials from Password Stores: Credentials from Web Browsers [T1555.003]

DCISE Reporting: Alert 26-011

Open-Source Reporting: https://arcticwolf.com/resources/blog/forticlient-ems-exploited-via-cve-2026-35616-to-deliver-ekz-infostealer-disguised-as-a-fortinet-patch/

MULTIPLE CISCO SD-WAN FLAWS EXPLOITED

Narrative: On 14 May 26, Cisco disclosed CVE-2026-20182 (CVSS score 10.0) affecting their Catalyst SD-WAN Controller. The vulnerability allows a remote attacker to bypass authentication and obtain administrator privileges for on-prem deployments, cloud configurations, and FedRAMP deployments. Cisco Talos associated the activity with UAT-8616. The threat actor attempted to add SSH keys, modify NETCONF configurations, and escalate root privileges in post-compromise activity.

Suspected Threat Actor: UAT-8616

CVE(s): CVE-2026-20182 (Improper Authentication), CVE2026-20245 (Improper Encoding/Escaping of Output)

TTP(s): Exploit Public-Facing Application [T1190], Account Manipulation: SSH Authorized Keys [T1098.004]

DCISE Reporting: Alert 26-017 and Alert 26-019

Open-Source Reporting: https://blog.talosintelligence.com/sd-wan-ongoing-exploitation/

PAN-OS GLOBAL PROTECT EXPLOITED

Narrative: On 29 May 26, Rapid7 published details regarding exploitation of CVE-2026-0257 (CVSS v4 score 7.8), an authentication bypass vulnerability, in Palo Alto's PAN-OS and Prisma Access. Exploitation allows a remote, unauthenticated attacker to forge authentication cookies and establish unauthorized virtual private network (VPN) connections. In June, Arctic Wolf reported an increase in this activity, with threat actors establishing IPSec tunnels and generating SMB and NTLM activity.

Suspected Threat Actor: Unknown

CVE(s): CVE-2026-0257 (Authentication Bypass)

TTP(s): Exploit Public-Facing Application [T1190], External Remote Services [T1133]

DCISE Reporting: Alert 26-018

Open-Source Reporting: https://www.rapid7.com/blog/post/etr-rapid7-observed-exploitation-of-pan-os-globalprotect-authentication-bypass-vulnerability-cve-2026-0257/