COLORTOKENS

THREAT INTELLIGENCE BRIEF #26

# ColorTokens Threat Advisory

June 30, 2026

ACCESS BRIEF

# Executive Summary

**Cyber Threat Intelligence (CTI) is critical in understanding and mitigating the evolving threats faced by various industries, like healthcare, finance & manufacturing industry.**

## HEALTHCARE

Healthcare organizations are frequent targets for cybercriminals due to the high value of patient data and the critical nature of their services. Ransomware attacks and data breaches can disrupt operations and risk patient safety by shutting down medical devices or hospital networks. CTI in healthcare helps identify threat actors, vulnerabilities in connected medical devices, and the latest attack tactics. By integrating CTI, healthcare providers can proactively strengthen defenses, protect sensitive data, and maintain patient care continuity.

## FINANCE

The finance sector faces continuous threats, including ransomware, Distributed Denial of Service (DDoS), and phishing attacks. Cybercriminals often target financial institutions to access valuable data or to extort money. CTI assists financial organizations in identifying emerging threats, such as new phishing tactics or advanced DDoS methods. By leveraging CTI, these organizations can better protect sensitive financial information, comply with regulations, and maintain trust with clients by preventing data breaches and financial losses.

## ACROSS SECTORS

Effective CTI helps these sectors stay ahead of adversaries by identifying threat actors, tactics, and indicators of compromise (IOCs).

SECTION 1

# Critical Vulnerability Information

**CVE-2026-12569**

## Remote Code Execution (RCE) vulnerability in Windchill PDMlink

**9.8 CRITICAL**
CVSS

A critical remote code execution (RCE) vulnerability has been reported in PTC Windchill PDMlink and PTC FlexPLM. The vulnerability may be exploited through the deserialization of untrusted data. * This advisory also applies to all CPS versions * The identified vulnerability also impacts Windchill and FlexPLM releases prior to 11.0 M030

### AFFECTED VERSIONS

Vendor : PTC
Product : Windchill PDMLink

affected from 0 through 11.0 M030
affected at 11.1 M020
affected at 11.2.1.0
affected at 12.0.2.0
affected at 12.1.2.0
affected at 13.0.2.0
affected at 13.1.0.0
affected at 13.1.1.0
affected at 13.1.2.0
affected at 13.1.3.0
Vendor

PTC

Product: FlexPLM

affected

affected from 0 through 11.0 M030
affected at 11.1 M020
affected at 11.2.1.0
affected at 12.0.0.0
affected at 12.0.2.0
affected at 12.1.2.0
affected at 12.1.3.0
affected at 13.0.2.0
aff

### PATCH DETAILS

https://www.ptc.com/en/support/article/CS473270

### Refrence

https://www.cve.org/CVERecord?id=CVE-2026-12569

**CVE-2026-20262**

## Cisco Catalyst SD-WAN Manager Arbitrary File Write Vulnerability

**8.0** HIGH CVSS

A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an authenticated, remote attacker to create a file or overwrite any file on the filesystem of an affected system. This vulnerability exists because the affected software does not properly validate user-supplied input during a file upload process. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected API endpoint of the affected system. A successful exploit could allow the attacker to create or overwrite any file on the underlying operating system. This file could later be used to elevate to root. To exploit this vulnerability, the attacker must have valid credentials with at least a lower-privileged, single-task user account.

### AFFECTED VERSIONS

Vendor:
Cisco

Product:
Cisco Catalyst SD-WAN Manager

Versions: 376 Total

Pleas check the link for the version list:
CVE Record: CVE-2026-20262

### PATCH DETAILS

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ

### Refrence

https://www.cve.org/CVERecord?id=CVE-2026-49448

**CVE-2026-35273**

## Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle

**9.8** CRITICAL CVSS

Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Updates Environment Management). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools

### AFFECTED VERSIONS

Affected Versions
>>Cisco Unified CM 12.5
All versions prior to 12.5SU9

>>Cisco Unified CM 14
All versions prior to 14SU6
>> Cisco Unified CM 15
All versions prior to 15SU5

### PATCH DETAILS

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW

### Refrence

https://www.cve.org/CVERecord?id=CVE-2026-20230

**CVE-2026-24858**

## Authentication Bypass vulnerability in Fortinet products.

**9.4** CRITICAL CVSS

An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.5, FortiAnalyzer 7.4.0 through 7.4.9, FortiAnalyzer 7.2.0 through 7.2.11, FortiAnalyzer 7.0.0 through 7.0.15, FortiManager 7.6.0 through 7.6.5, FortiManager 7.4.0 through 7.4.9, FortiManager 7.2.0 through 7.2.11, FortiManager 7.0.0 through 7.0.15, FortiNAC-F 7.6.3 through 7.6.5, FortiOS 7.6.0 through 7.6.5, FortiOS 7.4.0 through 7.4.10, FortiOS 7.2.0 through 7.2.12, FortiOS 7.0.0 through 7.0.18, FortiProxy 7.6.0 through 7.6.4, FortiProxy 7.4.0 through 7.4.12, FortiProxy 7.2.0 through 7.2.15, FortiProxy 7.0.0 through 7.0.22, FortiWeb 8.0.0 through 8.0.3, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4.0 through 7.4.11 may allow an attacker with a FortiCloud account and a registered device to log into other devices registered to other accounts, if FortiCloud SSO authentication is enabled on those devices.

### AFFECTED VERSIONS

Vendor : Oracle Corporation

Product: PeopleSoft Enterprise PeopleTools

affected
affected at 8.61
affected at 8.62

### PATCH DETAILS

https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

### Refrence

https://www.cve.org/CVERecord?id=CVE-2026-35273

**CVE-2026-8451, CVE-2026-8452**

## Memory overflow vulnerability leading to unpredictable or erroneous behaviour and Denial of Service

**9.8** CRITICAL CVSS

Memory overflow vulnerability NetScaler ADC and NetScaler Gateway leading to unpredictable or erroneous behaviour and Denial of Service if the appliance is configured as a Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server

### AFFECTED VERSIONS

Vendor: NetScaler

Product: ADC

affected
affected from 14.1 before 72.61
affected from 13.1 before 63.18
affected from 14.1 FIPS before 72.61
affected from 13.1 FIPS and NDcPP before 37.272

Vendor: NetScaler

Product: Gateway

affected
affected from 14.1 before 72.61
affected from 13.1 before 63.18

### PATCH DETAILS

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604

### Refrence

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604

**Note**

- The details provided about CVE vulnerabilities are based on publicly available sources, security advisories, and threat intelligence feeds. While efforts are made to ensure accuracy, the information may change over time.
- The severity scores (CVSS) and descriptions are for general reference. Organizations must conduct their own risk assessments based on their unique environment, configurations, and security posture.
- While patching and mitigation recommendations are provided, implementation decisions should be made based on an organization's security policies, compatibility testing, and vendor guidance.
- CVEs may be updated with new exploitation techniques or patches over time. Regular monitoring of official sources (e.g., NVD, MITRE, vendor advisories) is recommended.

SECTION 2

# Reported Cyber Breaches

HEALTHCARE

## Washington Dept. Health & Social Services Insider Breach Affects 8,600 Individuals

### ATTACK SUMMERY

The Washington Department of Social and Health Services (DSHS) has identified an insider data breach involving unauthorized access to the protected health information of approximately 8,600 individuals.

Insider threats are a major problem in healthcare, more so than in other sectors. While most insider incidents are unintentional, and snooping on medical records is a common cause of healthcare data breaches. DSHS employee was discovered to have accessed a DSHS internal client data system without authorization and viewed records containing full names, dates of birth, Social Security numbers, DSHS client numbers, and information about DSHS program enrolment.

The DSHS investigation found no evidence that health information was accessed, such as diagnoses, test results, treatments, claims, or chart notes. The DSHS said the employee was found to have accessed records for “reasons unrelated to their job duties,” but did not elaborate further on the individual’s reasons for access. It is also unclear when the unauthorized access was detected, or for how long the employee had been accessing records for non-work purposes.

DSHS confirmed that action was immediately taken when the privacy violations were identified, preventing further unauthorized access. DSHS has confirmed that the individual is no longer working for the department. It is unclear whether the employee was terminated over the HIPAA violation or if they left voluntarily.

DSHS said it is issuing notification letters by mail to all affected individuals and encourages them to monitor their account statements and credit reports for unauthorized activity. DSHS is cooperating with state and local law enforcement in their ongoing investigation. DSHS said steps are being taken to implement additional safeguards, and internal policies and procedures related to data privacy and security are being reviewed.

**References:**

- https://www.hipaajournal.com/washington-dept-health-social-services-insider-breach-2026/

HEALTHCARE

## Aitkin County Health and Human Services Data Breach

### ATTACK SUMMERY

Aitkin County Health and Human Services in Minnesota has identified a breach of its email environment. Data breaches have also been confirmed by Decatur Diagnostic Laboratory in Alabama and Gem State Dermatology in Idaho.

**Aitkin County Health and Human Services, Minnesota**

Aitkin County Health and Human Services in Minnesota has identified a breach of its email environment. On April 8, 2026, an email account was found to be sending phishing emails. Immediate action was taken to secure its email system, and an investigation was launched to determine the scope of the breach. Assisted by third-party digital forensics experts, Aitkin County HHS determined that there had been unauthorized access to three employee email accounts between April 7, 2026, and April 8, 2026. The investigation confirmed that the contents of one of the accounts had been downloaded.

The accounts were reviewed and found to contain the protected health information of 83,114 individuals, including names, addresses, dates of birth, Social Security numbers, dates of service, locations of service, individual case identifying numbers, PMI numbers, medical or health information, diagnosis and/or treatment information, healthcare provider names, medications, health insurance identification numbers, information regarding the type and status of forms filed with MnCHOICES, the date forms were last modified, health insurance claims information and/or information related to services received by Aitkin County HHS. A report containing some of the above data types relating to individuals not associated with the County was also found in the email account.

Passwords have been changed, employees have received additional training on email cybersecurity practices, and efforts are continuing to raise awareness of phishing emails. The email retention policy has also been updated to reduce the impact of any future incidents, and additional cybersecurity measures and monitoring partnerships are being considered to strengthen security.

**Decatur Diagnostic Laboratory, Alabama**

Decatur Diagnostic Laboratory Inc., in Alabama, has recently reported a data breach to the HHS' Office for Civil Rights using a placeholder estimate of at least 500 affected individuals. The clinical laboratory has added a breach notice to its website, which confirms that this was a hacking incident involving data exfiltration. The notice does not state when the breach was detected, or for how long the hacker had access to its network.

Decatur Diagnostic Laboratory has confirmed that the data exfiltrated in the attack included names in combination with one or more of the following: date of birth, Social Security number, driver's license number, medical record number, and/or patient code. The affected individuals have been advised to remain vigilant against incidents of identity theft and fraud over the next 24 months. The notice does not mention free credit monitoring and identity theft protection services. While this was not confirmed as a ransomware attack, a ransomware group has claimed responsibility. The LockBit 5 group claims it exfiltrated data in the attack and added the lab to its dark web data leak site.

**Gem State Dermatology, Idaho**

Improper disposal incidents are the rarest category of data breach. The first such incident of the year to date affects Gem State Dermatology in Boise, Idaho. On July 8, 2026, patient documents containing HIPAA-protected data were found in a dumpster three miles from the dermatology practice. A member of the public identified boxes of paperwork that appeared to be billing statements containing medical and personal information of patients of the dermatology practice. In addition to paperwork, what appeared to be thousands of microscope slides containing patient information, and presumably biological samples, were also found in the dumpster.

The material has now been collected by the practice, and an internal investigation has been launched to determine how the incident happened. At this early stage of the investigation, the practice is unable to confirm how any patients have been affected by the incident.

**References:**

- https://www.hipaajournal.com/aitkin-county-health-human-services-data-breach/

HEALTHCARE

## AdaptHealth Reports Material Cybersecurity Incident and Theft of Patient Data

### ATTACK SUMMERY

AdaptHealth, a publicly traded healthcare company that provides home medical equipment, diabetes supplies, and sleep therapy products, has informed the U.S. Securities and Exchange Commission (SEC) that it is investigating a material cybersecurity incident involving unauthorized access to patient data.

According to the company's Form 8-K filing, a threat actor contacted the company on June 15, 2026, claiming to have obtained files containing patient data. AdaptHealth launched an investigation, engaged third-party cybersecurity experts, and notified law enforcement. AdaptHealth has determined that certain cloud-based business applications were accessed by the threat actor, including internal patient management systems and document storage platforms. Files containing patients' personally identifiable information (PII) and protected health information were exfiltrated by the threat actor.

The investigation is ongoing; however, AdaptHealth has determined that the unauthorized access occurred as a result of a response to a social engineering attack on a third-party contractor, which allowed the contractor's credentials to be obtained. The threat actor obtained a stored password file tied to insurance billing and access to external electronic health record portals.

AdaptHealth said it considers this to be a material cybersecurity incident due to the nature and potential volume of data at risk. The financial impact of the incident is still being assessed, with the company potentially having to cover costs associated with forensics, breach notification, legal and regulatory responses, and any remediation measures. The company holds a cybersecurity insurance policy, which may cover certain losses associated with the incident.

While AdaptHealth has not named the threat actor behind the attack, this appears to have been a data theft and extortion attempt by the ShinyHunters threat group. ShinyHunters added AdaptHealth to its data leak site and has threatened to leak the stolen data if the ransom is not paid, giving the company a final warning to pay or face a data leak.

**References:**

- https://www.hipaajournal.com/adapthealth-data-breach/

TECH

## Windows BlueHammer flaw now exploited by ransomware gangs

### ATTACK SUMMERY

Dubbed BlueHammer, the security flaw (CVE-2026-33825) was leaked by a security researcher known as “Nightmare Eclipse” in early April, together with proof-of-concept exploit code, in protest at how the Microsoft Security Response Center (MSRC) handles the disclosure process.

“Insufficient granularity of access control in Microsoft Defender allows an authorized attacker to elevate privileges locally,” Microsoft explains in a security advisory. And, while the issue is not easy to exploit, it gives local attackers access to the Security Account Manager (SAM) database, which contains password hashes for local accounts.

With this access, they can escalate to SYSTEM privileges and potentially take complete control of the targeted system.

“At that point, [the attackers] basically own the system, and can do things like spawn a SYSTEM-privileged shell,”

Microsoft patched the vulnerability on April 14 as part of the April 2026 Patch Tuesday. However, days later, Huntress Labs security researchers revealed that threat actors had been exploiting it as a zero-day in attacks that showed evidence of “hands-on-keyboard threat actor activity.”

Over the past several months, Nightmare Eclipse has disclosed multiple other Windows zero-day exploits, including for the RoguePlanet, RedSun, GreenPlasma, MiniPlasma, YellowKey, and UnDefend flaws.

Some of these vulnerabilities affect Microsoft Defender, while others target BitLocker and Windows components.

Microsoft fixed the GreenPlasma, MiniPlasma, and YellowKey security flaws three weeks ago as part of the June 2026 Patch Tuesday updates.

**Flagged as exploited by ransomware gangs**

CISA added the BlueHammer flaw to its Known Exploited Vulnerabilities (KEV) Catalog on April 22, ordering Federal Civilian Executive Branch (FCEB) agencies to patch their Windows devices against ongoing CVE-2026-33825 attacks within two weeks, until May 7.

"This type of vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks to the federal enterprise," the U.S. cybersecurity agency warned at the time.

While Microsoft has yet to tag this security flaw as exploited in attacks, CISA has now also flagged it as exploited in ransomware campaigns in a Monday update to its KEV Catalog.

In recent years, CISA has flagged eight Microsoft Defender vulnerabilities that have been exploited in attacks, with two of them also targeted by ransomware gangs.

**References:**

- https://www.bleepingcomputer.com/news/security/cisa-windows-blueham-mer-flaw-now-exploited-by-ransomware-gangs/

TECH

## Fortinet Credential Harvesting Campaign Demonstrates Infrastructure-Scale Identity Risk

### ATTACK SUMMERY

FortiBleed is a clear warning for every organization that still depends on VPNs, perimeter devices, shared credentials, and broad administrative access to protect critical environments.

Global cybersecurity agencies have warned that attackers are targeting internet-facing Fortinet firewalls and VPN gateways using compromised credentials. The campaign, known as FortiBleed, reportedly involves leaked credentials associated with approximately 74,000 Fortinet devices, including firewalls and VPN gateways. Other reporting estimates the scope may be even higher, with researchers identifying more than 86,000 confirmed working credentials across 194 countries.

The most important point is that FortiBleed is not being described as a new Fortinet zero-day. Fortinet has said the activity is tied to credential harvesting, brute-force activity, and data from previous incidents — not a new advisory or recent incident.
Attackers do not always need to exploit a new vulnerability. If they have valid credentials, they can simply log in.

### What Makes FortiBleed So Concerning

FortiBleed appears to reflect a broader shift in attacker behavior: stolen identities are becoming the path of least resistance.

According to public reporting, researchers found evidence of password theft affecting Fortune 500 companies and government agencies across more than 15 countries. Hudson Rock described the scale as “staggering,” and Reuters reported that the campaign potentially gave attackers a way to penetrate deeper into affected organizations and steal data.

Agencies in the U.S., U.K., and Australia warned that attackers are actively targeting internet-facing Fortinet devices with compromised credentials, allowing them to bypass perimeter defenses and gain direct entry into enterprise networks.

This is what makes FortiBleed different from a traditional vulnerability story. The firewall is not simply the thing being attacked. It becomes the access path.

Once credentials work, attackers may be able to reach VPN portals, administrative interfaces, internal systems, Active Directory environments, and other high-value resources. That turns credential exposure into a breach-containment problem.

**References:**

- https://xage.com/blog/fortibleed-shows-why-stolen-credentials-must-never-become-a-master-key/

SECTION 3

# OT/IoT Security Breaches

OT & IOT

## Tata Electronics hit by cyber breach claiming to expose Apple, Tesla trade secrets

### ATTACK SUMMERY

Tata Electronics said it had detected a recent “cybersecurity incident”, after researchers said World Leaks posted purported component design and specification papers of Apple and Tesla, both customers of the Indian group.

The ransomware group has posted more than 200,000 files on the dark web, the security researchers told Reuters.

Apple was investigating the breach and a “full analysis was going on”, a source familiar with the matter said, adding that Tata had received a ransom demand related to the incident.Apple (AAPL.O), opens new tab did not respond to requests for comment. Tata Electronics declined to comment on the ransom demand.

The breach is the latest setback for Apple’s supply chain in India, where Tata faces scrutiny over alleged contamination of farmlands near one of its iPhone parts plants, Reuters reported.

Tata is emerging as one of Apple’s most important manufacturing partners outside China, an expansion that is a cornerstone of Prime Minister Narendra Modi’s push to make India an electronics manufacturing powerhouse.

Tata was hit by a cyberattack on its British Jaguar Land Rover group last year that resulted in a six-week output halt.

The Indian Computer Emergency Response Team, a unit under India’s IT ministry that oversees cyber incidents, did not immediately respond to Reuters emails seeking comment.

### APPLE ‘FACTORYDATA’

World Leaks, which has previously claimed responsibility for a Nike break-in, said on its dark net website that it was publishing stolen data from Tata Electronics.

Reuters could not immediately verify the authenticity of the data and could not immediately reach World Leaks for comment.

The World Leaks website says the Tata Electronics data comprises more than 200,000 files totalling over 630 gigabytes. A database on its website shows several purported Apple files and folders, some titled “com.apple.factorydata”, and documents referring to “material specification”.

Indian cybersecurity researcher Rajshekhar Rajaharia, who reviewed the Tata files on World Leaks for Reuters, said they also contain emails, event logs spanning several years and passport copies of employees including foreign nationals.

Rajaharia has previously advised Indian police on cyber incidents.

The website is only accessible on the dark web, or dark net, beyond the reach of search engines. A second security researcher who reviewed the data dump, Rakesh Krishnan, told Reuters it had been accessible on the dark web since at least June 10.

TESLA DOCUMENTS, ‘TRADE SECRET’

Tata also makes parts for Tesla, industry sources say.

One folder on the World Leaks database was labelled “NV36 Chargeport Controller - North America”, a purported reference to parts used in an upgraded version of Tesla’s Model Y SUV.

Another purported Tesla 2023 document described as “TRADE SECRET” showed certain drawings for its project Highland - a publicly known internal codename for its revamped Model 3 sedan. Rajaharia also shared a screen recording of his review of the files. It showed a search for “Apple” returned 181 files and folders, while a search for “Tesla” returned files including what appeared to be manufacturing specifications and an assembly document dated May 2025.

Some files published by World Leaks carried footers saying, “This document contains proprietary and confidential information of Apple Inc.” and “information contained herein is deemed confidential, proprietary, and a trade secret of Tesla Inc.”

The breach highlights the vulnerability of global businesses to increasingly sophisticated cyber and ransom attacks.

Among the files was a 52-page document bearing Apple’s proprietary markings purportedly detailing quality inspection standards for iPhone circuit board components. There were also 33 files and folders for search term “Hosur” - the location of Tata’s main iPhone assembly plant in Tamil Nadu state.

Tata informed some employees at its iPhone assembly operations last week of the data breach, said a second industry source familiar with the matter.

**References:**


- https://www.reuters.com/business/media-telecom/indias-tata-electronics-hit-by-cyber-breach-claiming-expose-apple-tesla-trade-2026-06-22/

## DISCLAIMER

“Cyber threats are constantly evolving, and the tactics, techniques, and procedures (TTPs) described in this report may change over time. Continuous monitoring and threat intelligence updates are recommended to maintain an effective security posture.”

## FEEDBACK

“We welcome your feedback to enhance the accuracy, relevance, and effectiveness of our threat intelligence reports. Please share your insights or recommendations to help us improve future editions and better support your security needs.”

**Contact us on - Threat Advisory (threatadvisory@colortokens.com)**

---

### About ColorTokens:

ColorTokens is a leading provider of enterprise microsegmentation solutions that operationalize breach readiness across hybrid, cloud, and OT environments. By proactively minimizing lateral movement risk and reducing attack surface, ColorTokens enables organizations to operate in a continuous state of breach readiness — before, during, and after an incident. The Xshield™ platform visualizes traffic between workloads, OT/IoT/IoMT devices, and users, enforcing adaptive micro-perimeters that dynamically limit blast radius and accelerate response. Recognized as a Leader in The Forrester Wave™: Microsegmentation Solutions (Q3 2024) and the GigaOm Radar for Microsegmentation v3 (March 2026), ColorTokens helps enterprises strengthen operational resilience and maintain security posture as threats evolve. For more information, visit www.colortokens.com.

Copyright 2026 © ColorTokens. All rights reserved.