SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

March 2026 - VOL.4

The News

IN THE NEWS THIS WEEK

Oracle Patches Critical CVE-2026-21992 Enabling Unauthenticated RCE in Identity Manager

Oracle has released security updates to address a critical security flaw impacting Identity Manager and Web Services Manager that could be exploited to achieve remote code execution.

The vulnerability, tracked as CVE-2026-21992, carries a CVSS score of 9.8 out of a maximum of 10.0.

"This vulnerability is remotely exploitable without authentication," Oracle said in an advisory. "If successfully exploited, this vulnerability may result in remote code execution."

According to a description of the flaw in the NIST National Vulnerability Database (NVD), it's "easily exploitable" and could allow an unauthenticated attacker with network access via HTTP to compromise Oracle Identity Manager and Oracle Web Services Manager. This, in turn, can result in the successful takeover of susceptible instances.

Oracle makes no mention of the vulnerability being exploited in the wild. However, the tech giant has urged customers to apply the update without delay for optimal protection.

READ MORE

OTHER NEWS HIGHLIGHTS

Trivy Hack Spreads Infostealer via Docker, Triggers Worm and Kubernetes Wiper

TeamPCP Backdoors LiteLLM Versions 1.82.7–1.82.8 via Trivy CI/CD Compromise

Eight Attack Vectors Inside AWS Bedrock.

The News

TOP OF THE NEWS THIS WEEK

iOS, macOS 26.4 Roll Out With Fresh Security Patches

Apple on Tuesday rolled out a fresh wave of security updates to resolve more than 80 vulnerabilities across its mobile and desktop operating systems.
iOS 26.4 and iPadOS 26.4 were released for the latest generation iPhone and iPad devices with patches for nearly 40 security defects.
WebKit received fixes for eight bugs that could be exploited by malicious websites to bypass policy enforcement, mount XSS attacks, fingerprint users, escape the sandbox, or crash the process.
Issues addressed in the kernel could be exploited to disclose kernel memory, leak sensitive kernel state, corrupt kernel memory, or write kernel memory.
Vulnerabilities resolved in other components may lead to network traffic interception, access to biometrics-gated Protected Apps, process crashes, app termination, denial-of-service (DoS), installed apps enumeration, sandbox escape, and access to sensitive information.
Patches for roughly two dozen of these security defects were delivered to users of older devices as part of the iOS 18.7.7 and iPadOS 18.7.7 security updates.

READ MORE

TOP RELATED ARTICLES

Critical Citrix NetScaler Vulnerability Poised for Exploitation, Security Firms Warn

Chrome 146 Update Patches High-Severity Vulnerabilities

Hackers Exploit CVE-2025-32975 (CVSS 10.0) to Hijack Unpatched Quest KACE SMA Systems

Geo-Politics

NEWS FROM AROUND THE WORLD

Iran Built a Vast Camera Network to Control Dissent. Israel Turned It Into a Targeting Tool

Hundreds of millions of cameras have been installed above shops, in homes and on street corners across the world, many connected to the internet and poorly secured. Recent advances in artificial intelligence have enabled militaries and intelligence agencies to sift through vast amounts of surveillance footage and identify targets.

On Feb. 28, Israel vividly demonstrated the potential of such systems to be hacked and used against adversaries when Israel tracked down Iranian leader Ayatollah Ali Khamenei with the help of Tehran's own street cameras – despite repeated warnings that Iran's surveillance systems had been compromised, according to interviews and an Associated Press review of leaked data, public statements and news reports.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

North Korean Hackers Abuse VS Code Auto-Run Tasks to Deploy StoatWaffle Malware

Iranian hackers targeting opponents with Telegram malware

Iran Hacktivists Make Noise but Have Little Impact on War

Breaches

SECURITY BREACHES THIS WEEK

Extortion Group Claims It Hacked AstraZeneca

The hackers say they exfiltrated multiple types of sensitive enterprise data from AstraZeneca, including credentials and tokens, internal code repositories, and employee data.

Lapsus$ claims to have exfiltrated Java-based application code such as “controllers, repositories, services, schedulers, configuration files, and Spring Boot resources,” cybersecurity firm SocRadar reports.

The leak allegedly includes project paths associated with internal development assets, Angular and Python packages, and AWS, Azure, and Terraform cloud infrastructure information.

Furthermore, the hackers claim to have stolen various credentials and other secrets, GitHub Enterprise-related user information, such as roles and account details, and corporate email addresses.

“The file tree also points to large numbers of SQL scripts, table definitions, views, sequence files, batch processes, and inventory or order-management components,” SocRadar notes.

READ MORE

OTHER SECURITY BREACHES

HackerOne Employee Data Exposed in Massive Navia Breach

TeamPCP Hacks Checkmarx GitHub Actions Using Stolen CI Credentials

Dutch Finance Ministry Blocks Computer Systems After Hack

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-21992 - Critical Vulnerability in Oracle Identity Manager and Web Services Manager

CVSS SCORE 9.8

CVE-2026-3055 - NetScaler Vulnerability Poised for Exploitation

CVSS SCORE 9.3

LAST WEEKS RECAP

CVE-2026-20131 Cisco Secure Firewall Management Center Software Remote Code Execution Vulnerability
CVSS Score: (10.0)

CVE-2026-32746 Telnet: Critical vulnerability allows injecting malicious code from the network
CVSS Score: (9.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

A total of 138 new victims were reported across various ransomware groups this Week.

TARGET INDUSTRIES

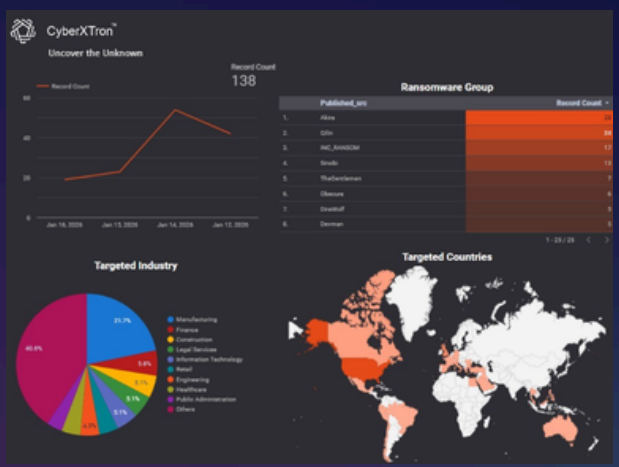
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

TARGET COUNTRY

The USA was the top victim country, with a total of 76 affected entities.

TOP GROUP

The Akira was the most active, claiming 28 victims.



Dive into this interactive report to uncover hidden trends HERE!

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

TOP THREAT ACTORS

Qilin

Qilin is a ransomware-as-a-service operation linked to Russia, encrypting and stealing data for ransom. Active since October 2022, it has targeted organizations like The Big Issue and Yanfeng.

Akira

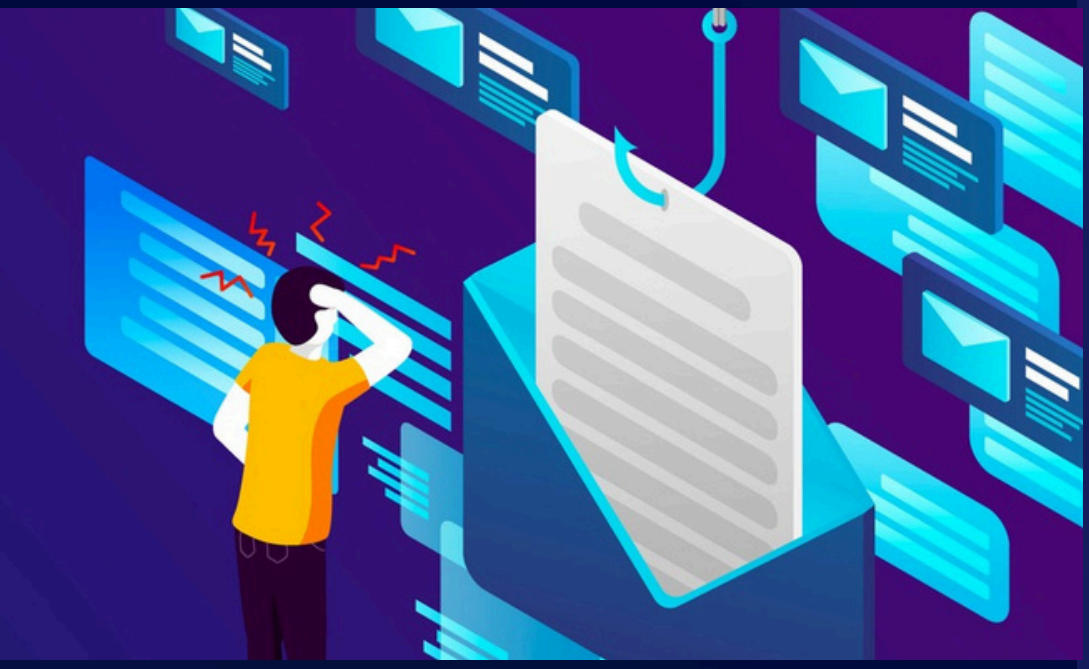
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

Clop

Clop ransomware first emerged in 2019, when it became a prevalent threat to organizations and businesses. Clop ransomware encrypts the victims files and threatens to leak the confidential information if no ransom is paid.

Phishing

PHISHING NEWS THIS WEEK



An AI-powered phishing campaign has compromised hundreds of organizations

A phishing campaign tied to AI cloud-hosting service Railway has given hackers access to the Microsoft cloud accounts for hundreds of businesses, according to researchers at Huntress.

Rich Mozeleski, product manager for Huntress' identity team, told CyberScoop the campaign is currently tied to a smaller actor and approximately a dozen IP addresses, but has managed to compromise hundreds of targets in the past few weeks.

In early March it was compromising a few dozen targets a day, but starting March 3, there was a "massive increase" in that tempo. Mozeleski said that in addition to being more sophisticated than usual, there were no identical emails or domains used, leading researchers to suspect that they may have been generated through artificial intelligence tools. The templates ranged from traditional email lures to QR codes and co-opted file-share sites.

READ MORE

OTHER PHISHING ARTICLES

Microsoft warns tax pros that they're phishing targets

New Npm 'Ghost Campaign' Uses Fake Install Logs to Hide Malware

Tycoon2FA Phishing Service Resumes Activity Post-Takedown