

INTELLIGENCE BRIEF

November 2026 Threat Watch

As of November 3, a new WordPress exploitation listing joins VPN exposure and identity abuse on the defender agenda. Prioritize exposed systems, verified account recovery, and control of connected apps.

EDITION

Fall/Winter 2026/2027 Edition

TR-02 · Technology risk

PUBLISHED BY

Z7 Solutions LLC

Orlando, Florida

READ ONLINE

z7solutions.com

844-974-8669

01 At a Glance

STATUS

ONGOING RISK

Official exploitation records and identity guidance reviewed November 3, 2026; underlying events retain their own dates.

HEADLINE NUMBERS

3
Defensive priorities in this watch

Nov 3
2026 source review date

KEY FACTS

REVIEWED
November 3, 2026

NEW CATALOG ENTRY
WordPress CVE-2026-119977, November 3 [1]

VPN EXPOSURE
Ivanti Connect Secure vulnerability chain [1]

IDENTITY PATTERN
Impersonated IT staff, followed by SaaS data theft [3]

APP ACCESS
Consent grants require a separate security review [4]

02 What Happened

Today's WordPress exploitation listing puts public applications on the November agenda. Z7's three priorities are exposed systems, verified account recovery, and app access. [1]

- WordPress released version 7.1.4 on October 28, fixing an upgrade-process weakness that can permit remote code execution. Confirm the security update on every site you operate or outsource. [2]
- CISA's October 30 Ivanti entries link CVE-2026-118527 and CVE-2026-111357 with CVE-2026-104935. Review the complete vendor remediation. [1]

- Google documented January 2026 calls impersonating IT staff, stolen sign-on credentials and MFA codes, and unauthorized MFA device enrollment before cloud data theft. These are dated observations, not newly reported November incidents. [3]
- Microsoft guidance updated October 21 explains a different route: a user can grant a malicious app access through a legitimate consent screen. A trusted sign-in domain does not establish that the app deserves access. [4]

03 How It Works

01 Reach the exposed system

WordPress documents an upgrade-process route to code execution. Z7 recommends matching every public service to its owner and applicable advisory. [2]

02 Persuade the account holder

An alternative route starts with an apparent IT support call. In Google's January cases, the caller obtained credentials and MFA codes and added another MFA device. [3]

03 Use the resulting authority

A compromised session can reach the SaaS applications available to that user. A consented app can separately exercise its granted data permissions. These are distinct access paths. [3, 4]

04 Create a data-loss incident

Google observed cloud data theft supporting extortion. Defenders need both an access investigation and an assessment of which records left the tenant. [3]

04 Who Is at Risk

Exposure follows the systems and permissions you actually operate. This is a defensive selection, not a global victim ranking.

- Website owners relying on hosting agencies to manage WordPress updates. [2]
- Organizations with the Ivanti products named in the catalog entries. [1]
- Cloud users who can be persuaded to change authentication or approve unfamiliar applications. [3, 4]

Sectors in scope: Organizations operating public WordPress sites, Organizations using Ivanti Connect Secure, Employers and service providers using cloud identity and SaaS.

05 What Changed Since the Last Edition

EACH CHANGE WITH ITS SOURCE

01 November 3: CISA added the WordPress issue, with a November 6 catalog remediation date. Private organizations should determine their applicable requirements.

SOURCE 1

02 October 28: WordPress issued the security release that addresses the upgrade-process weakness.

SOURCE 2

03 October 21: Microsoft updated its consent-phishing guidance, including how to investigate suspicious applications.

SOURCE 4

06 What to Do Now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Assign owners to the public sites and VPNs in your inventory.**

Compare actual exposure with the catalog and product guidance; confirm outsourced systems with their operators. [1, 2]

02 **Complete the WordPress security update and verify the result.**

The vendor recommends immediate updating; retain the installed version and change record as evidence. [2]

03 **Review the entire Ivanti advisory for affected appliances.**

The catalog links multiple vulnerabilities; confirm the complete vendor remediation with the appliance owner. [1]

04 **Rehearse a suspicious support call with the help desk.**

Z7 recommends independent verification before changing authentication, plus phishing-resistant MFA where supported, based on the observed call-to-enrollment sequence. [3]

05 **Investigate unfamiliar app grants and preserve the logs.**
Microsoft recommends reviewing permissions, application audit activity, and user sign-ins; scope affected data before closing the incident. [4]

07 Indicators

Indicators the sources publish, as they print them. Hunt with them, and check the source before you block.

BEHAVIOR A caller claiming to be IT requests an MFA update, followed by an unfamiliar authentication device. [3]

BEHAVIOR Unexpected application permissions or suspicious application activity in Entra audit and sign-in logs. [4]

08 Sources

[1] **Known Exploited Vulnerabilities Catalog, version 2026.11.03** CISA · November 3, 2026. https://raw.githubusercontent.com/cisagov/kev-data/develop/known_exploited_vulnerabilities.json

[2] **WordPress 7.1.4** WordPress · October 28, 2026. https://wordpress.org/news/2026/10/wordpress-7-1-4/

[3] **Vishing for Access: Tracking the Expansion of ShinyHunters-Branded SaaS Data Theft** Google Threat Intelligence Group · January 30, 2026. https://cloud.google.com/blog/topics/threat-intelligence/expansion-shinyhunters-saas-data-theft

[4] **Protect against consent phishing** Microsoft · Updated October 21, 2026. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/protect-against-consent-phishing

NEXT STEP

What does this mean for your security?

Bring your questions about November 2026 defensive priorities, your environment and the controls you rely on. Talk through the most useful next step with Z7 Solutions LLC.

01 / Exposure

Bring one question about how this threat could affect your environment.

02 / Priorities

Bring your current safeguards, open gaps and budget questions.

ALSO IN THIS EDITION

Post-quantum deadlines set, attack estimates fall
More from the edition · z7solutions.com/z7-cyber/quantum-era/

Qilin still tops most ransomware counts
More from the edition · z7solutions.com/z7-cyber/qilin/

Qilin still hits hospitals and infrastructure
More from the edition · z7solutions.com/z7-cyber/qilin-part-2/

CALL 844-974-8669

EMAIL sales@z7solutions.com

BOOK A SECURITY CONVERSATION Book a Security Conversation ↗

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.