

NSA and Partners Alert Zimbra Collaboration Suite Users of a Russian State-Supported Phish

Published: 2026-07-23 · Archived: 2026-07-25 02:01:56 UTC



NSA and Partners Alert Zimbra Collaboration Suite Users of a Russian State-Supported Phishing Campaign

PHOTO INFORMATION

FORT MEADE, Md. (July 23, 2026) — Today, the National Security Agency (NSA) in collaboration with partners, is releasing a Cybersecurity Advisory (CSA) titled, [“Russian State-Supported Cyber Actors Conduct Phishing Campaign Targeting Users of Zimbra Collaboration Suite.”](#)

Since July 2025, the Russian state-supported advanced persistent threat group known as LAUNDRY BEAR has utilized phishing emails to target the Zimbra Collaboration Suite (ZCS) across various U.S. and allied government and commercial networks. Supported by a custom-developed capability named “Ulej,” the actors leverage a view-based exploit that triggers automatically when a user views a malicious email within a vulnerable version of the webmail service. This exploited a zero-day vulnerability (CVE-2025-66376) when it was first used by the threat group and is still used to successfully exploit ZCS instances that are still unpatched. The exploit attempts to exfiltrate the organization’s email directory, the last 90 days of the victim’s communications, and other sensitive information to servers controlled by the actors.

The joint CSA characterizes the network activity occurring during the exfiltration stage and documents observed indicators of compromise (IOCs) to help organizations develop robust detection and mitigation capabilities. The report also provides specific remediations steps for organizations that discover the presence of the listed IOCs.

Co-sealing agencies include the Federal Bureau of Investigation (FBI), Netherlands Defence Intelligence and Security Service (MIVD), Netherlands General Intelligence and Security Service (AIVD), Cybersecurity and Infrastructure Security Agency (CISA), Defense Counterintelligence and Security Agency (DCSA), Department of Defense Cyber Crime Center (DC3), Department of the Treasury, Naval Criminal Investigative Service (NCIS), Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC), Communications Security Establishment Canada’s (CSE’s) Canadian Centre for Cyber Security (Cyber Centre), New Zealand National Cyber Security Centre (NCSC-NZ), United Kingdom National Cyber Security Centre (NCSC-UK), Czech Republic National Cyber and Information Security Agency (NÚKIB), Danish Defence Intelligence Service (DDIS), Estonian Foreign Intelligence Service (EFIS), Finnish Defence Intelligence (FDI), Finnish Security and Intelligence Service (SUPO), French General Directorate for Internal Security (DGSI), French National Cybersecurity Agency (ANSSI), Italian External Intelligence and Security Agency (AISE), Italian Internal Intelligence and Security Agency (AISI), Security and Intelligence Service of the Republic of Moldova (SIS RM), Polish Foreign Intelligence Agency (AW), The Military Counterintelligence Service of Poland (SKW), Spain National Intelligence Centre (CNI), Sweden National Cyber Security Centre (NCSC-SE).

Additional Resources

[Read the full report](#)

.

[Visit our full library for more cybersecurity information and technical guidance](#)

.

NSA Media Relations

MediaRelations@nsa.gov

443-634-0721

About the National Security Agency.

Founded in 1952, NSA is a U.S. Department of War combat support agency and element of the U.S. Intelligence Community. The Agency's mission is to provide foreign signals intelligence to policy makers and our military, and to prevent and eradicate cybersecurity threats to U.S. National Security Systems, with a focus on the Defense Industrial Base and the improvement of U.S. weapons security. From protecting U.S. warfighters around the world to enabling and supporting operations on land, in the air, at sea, in space, and in the cyber domain, NSA is committed to building public trust through transparency and protecting civil liberties and privacy consistent with our nation's values.

###

Source: <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4553352/nsa-and-partners-alert-zimbra-collaboration-suite-users-of-a-russian-state-supp/>