ALLIANCE OF SCHOOLS FOR COOPERATIVE INSURANCE PROGRAMS

ASCIP

On the Alert!

Date: November 30, 2021

Attention: ASCIP Members

Affected: Administrators, Legal, Risk Management, Faculty & Staff

Applicability: K-12, Community Colleges & Charter Schools

ZOHO SOFTWARE BREACH

As of November 8, 2021, hackers have exploited a **Zoho** software vulnerability at nine organizations across several sectors, including the education sector.

The exploited flaw in the sign-on and password management software allows them to take over vulnerable systems on an organization's network. With the help of the National Security Agency (NSA), cybersecurity researchers are exposing ongoing efforts by these unidentified hackers.

Tracking the threat

Officials from the NSA and US Cybersecurity & Infrastructure Security Agency (CISA) are tracking the threat. The NSA and CISA declined comment on the identity of the hackers. According to preliminary disclosures by the NSA and DHS, the threat actors are based out of China. Federal officials continue to work closely with cybersecurity firms to stay on top of the threats. Palo Alto Networks stated that some of the attackers' tactics and tools overlap with those used by a suspected Chinese hacking group.

Stolen passwords to maintain long-term access

According to senior Palo Alto Networks executive Ryan Olson, the threat-actors have obtained passwords from some targeted organizations with the goal of maintaining long-term access to those networks. This enables the threat actors to be well-placed to intercept sensitive data sent over email or browse for credentials stored on computer systems until they are detected and removed from the network. Olson said that the nine confirmed victims are "the tip of the spear".

Cybersecurity firm, Mandiant, revealed earlier this year that China-linked hackers had been exploiting a different software vulnerability to breach defense, financial, and public sector organizations in the US and Europe. Palo Alto Networks also revealed that in the activity monitored, threat-actors are exploiting a vulnerability in software which corporations use to manage their network passwords, such as OneLogin, PassBolt, or LastPass

Suggested threat detection

If your district uses Zoho software, Information Technology (IT) Directors & Professionals are encouraged to update their systems and look for signs of a breach. ASCIP can assist members take a proactive approach be conducting a risk and vulnerability assessment. In addition, should a member fall victim of a breach, ASCIP can help in the mitigation process by acquiring the necessary resources and minimize the impact. Please contact ASCIP to inquire about ASCIP's Cyber Services Program.

Please contact your ASCIP Risk Services Consultant or our Risk Services team at RM_Info@ascip.org for questions or to discuss further.