

# FBI/DHS: Government election systems face threat from active ZeroLogon exploits

Getty Images

## reader comments

29 with 25 posters participating

## Share this story

The FBI and the cybersecurity arm of the Department of Homeland Security said they have detected hackers exploiting a critical Windows vulnerability against state and local governments and that in some cases the attacks are being used to breach networks used to support elections.

Members of unspecific APTs—the abbreviation for advanced persistent threats—are exploiting the Windows vulnerability dubbed ZeroLogon. It gives attackers who already have a foothold on a vulnerable network access to the all-powerful domain controllers that administrators use to allocate new accounts and manage existing ones.

To gain initial access, the attackers are exploiting separate vulnerabilities in firewalls, VPNs, and other products from companies including Juniper, Pulse Secure, Citrix NetScaler, and Palo Alto Networks. All of the vulnerabilities—ZeroLogon included—have received patches, but as evidenced by Friday's warning from the DHS and FBI, not everyone has installed them. The inaction is putting governments and elections systems at all levels at risk.

Officials wrote:

*This recent malicious activity has often, but not exclusively, been directed at federal and state, local, tribal, and territorial (SLTT) government networks. Although it does not appear these targets are being selected because of their proximity to elections information, there may be some risk to elections information housed on government networks.*

*CISA is aware of some instances where this activity resulted in unauthorized access to elections support systems; however, CISA has no evidence to date that integrity of elections data has been compromised. There are steps that election officials, their supporting SLTT IT staff, and vendors can take to help defend against this malicious cyber activity.*

ZeroLogon works by sending a string of zeros in a series of messages that use the Netlogon protocol, which Windows servers rely on for a variety of tasks, including allowing end users to log in to a network. People with no authentication can use the exploit to gain domain administrative credentials, as long as the attackers have the ability to establish TCP connections with a vulnerable domain controller. The requirement to establish TCP connections with the domain controller is likely why attackers are chaining ZeroLogon with exploits of VPNs and firewalls.

Friday's advisory provides some guidance for organizations that think they have or may have been compromised. The most important takeaway is that the targeted vulnerabilities—some that have been available for more than a year — should be applied or the hardware they run should be disconnected from their networks.

<https://arstechnica.com/?p=1713241>