Cisco and Palo Alto Networks Appliances Impacted By Kerberos Authentication Bypass

Cisco and Palo Alto Networks have fixed similar high-risk authentication bypass vulnerabilities in their network security devices that were caused by an oversight in the implementation of the Kerberos protocol.

Man-in-the-middle (MitM) attackers could exploit these weaknesses to get administrative control over the appliances.

Researchers from security firm Silverfort discovered both vulnerabilities, which are similar and could potentially exist in other Kerberos implementations. Cisco patched the flaw earlier this month and Palo Alto Networks this week.

Kerberos vulnerabilities

The vulnerability in PAN-OS, the operating system that runs on network security devices and appliances from Palo Alto Networks, is tracked as CVE-2020-2002 and is rated high risk.

The flaw exists in PAN-OS 7.1 versions earlier than 7.1.26, PAN-OS 8.1 versions earlier than 8.1.13, PAN-OS 9.0 versions earlier than 9.0.6, and all versions of PAN-OS 8.0. PAN-OS 8.0 has reached end-of-support and did not receive an update.

"An authentication bypass by spoofing vulnerability exists in the authentication daemon and User-ID components of Palo Alto Networks PAN-OS by failing to verify the integrity of the Kerberos key distribution centre (KDC) before authenticating users," the company said in its advisory.

"This affects all forms of authentication that use a Kerberos authentication profile. A man-in-the-middle type of attacker with the ability to intercept communication between PAN-OS and KDC can login to PAN-OS as an administrator."

A similar vulnerability, tracked as CVE-2020-3125, exists in the Cisco Adaptive Security Appliance (ASA) Software and was patched on May 6. Devices running Cisco ASA Software are affected if they have Kerberos authentication configured for VPN or local device access.

Cisco's advisory contains manual instructions for administrators to check if Kerberos authentication is configured, as well as a table with fixed Cisco ASA versions. However, the company warns that addressing this issue requires making some configuration changes even after the software has been updated.

"Cisco ASA devices are vulnerable and can still be exploited unless the CLI commands validate-kdc and aaa kerberos import-keytab are configured," Cisco said. "These new configuration commands ensure that the ASA validates the KDC during every user authentication transaction, which prevents the vulnerability that is described in this security advisory."

Impersonating the Kerberos KDC

Kerberos is a popular authentication protocol in enterprise active directory environments. However, to provide maximum security the protocol has three authentication steps: The user authenticates to the server, the server authenticates to the client, and the Kerberos KDC authenticates to the server.

"Apparently, KDC authentication to the server is often overlooked," the Silverfort researchers said in a blog post. "Perhaps because requiring it complicates the configuration requirements. However, if the KDC does not authenticate to the server, the security of the protocol is entirely compromised, allowing an attacker that hijacked the network traffic to authenticate to PAN-OS with any password, even a wrong one."

Kerberos KDC spoofing is not actually a new attack and was first reported ten years ago by a security researcher named Dug Song. This suggests that both the Cisco ASA and Palo Alto PAN-OS implementations have been vulnerable for a long time.

The Silverfort researchers discovered the oversight while trying to implement a multi-factor authentication solution compatible with third-party security appliances.

The company has the following recommendations for any developers implementing Kerberos:

Validate that the implementation of Kerberos requires a password or keytab: To validate the DC, you need to use some kind of shared secret. If your solution does not enable configuring a keytab file, or a service account password, the application is surely susceptible to KDC spoofing

Run Wireshark: Use Wireshark to see what Kerberos requests are sent during authentication. If there is no TGS_REQ, itâ€™s a red flag

Follow protocol RFCs: If you want to implement an authentication protocol yourself, you must follow the protocol RFCs diligently. Silverfort recommends taking the easier route and use an existing implementation of these protocols

Use third-party libraries properly: Some third-party libraries require specific configuration to avoid KDC spoofing. For example, a common library used for Kerberos called pam-krb5, has to have a keytab configured to work properly

References:

- https://www.csoonline.com/article/3543838/cisco-and-palo-alto-networks-appliances-impacted-by-kerberos-authentication-bypass.html?&web_view=true
- https://www.arnnet.com.au/article/679722/cisco-palo-alto-networks-appliances-impacted-by-kerberos-authentication-bypass/
- https://www.oodaloop.com/cyber/2020/05/15/cisco-and-palo-alto-networks-appliances-impacted-by-kerberos-authentication-bypass/
- https://blog.deepwatch.com/palo-alto-networks-cisco-kerberos-authentication-bypassa