ArrayOS TM Security Advisory for CVE-2008-4609

Date: - October 9, 2009

Overview

The security advisory is Array Networks response to CVE-2008-4609 (CERT-FI: FICORA #193744) security vulnerability. The advisory states that the general impact of the attack scenarios is a Denial of Service (DoS). These attacks aim to create a DoS condition for a specific service by opening a large number of TCP connections and/or by sending an excessive amount of specially-crafted packets with the TCP receive window set to a small or zero value. Array OS mitigates DoS attacks by employing number of defense in depth countermeasures to protect target services on Array Networks systems running Array OS software.

Mitigation

Our internal testing showed Array OS can mitigate the majority of DoS attacks mentioned in the CERT-FI's advisory.

NOTE: - In the interest of following best security practices, Array Networks recommends using mitigation measures to effectively deal with DoS attacks. The mitigation steps are sufficient to mitigate the risk.

a. Configure an access control list rule such that only trusted and known hosts that are inside the network perimeter can access the management interface of the Array appliance when using WebUI or SSH. This will prevent the attacker from attacking the management interface of the Array appliance.

(config)# accesslist permit tcp [Trusted host IP address] 255.255.255.255 0 [Management IP of the Array appliance] 255.255.255.255 [Mgmt/SSH port] [Access list ID]
(config)# webwall [Interface name] on
(config)# accessgroup [Access list ID] [Interface name]

b. During the DoS traffic attack (that initiate's large number of TCP connections to Array services), virtual services on the Array appliances will stay running and the system will not crash or reboot. Customers can keep the services available for the general traffic during the attack by configuring a low TCP idle timeout, which will effectively terminate DoS TCP connections. Once the attacker source IP address is identified customers can configure an accesslist rule to deny all the TCP traffic from the attacker and completely preventing the attacker from consuming Array appliance resources.

Configuring the tcpidle timeout to 60 seconds, the lowest available

(config)#system tune tcpidle 60

Configuring the access list rule to prevent all traffic from the attacker IP once the attacker is identified

(config)# accesslist deny tcp [Attacker IP address/range] [Netmask] 0 [Virtual service IP address on the Array appliance] [Virtual service netmask] [Virtual service port] [Access list ID]
(config)# webwall [Interface name] on
(config)# accessgroup [Access list ID] [Interface name]

c. The DoS attack specified cannot establish SSL connections as per the CERT-FI advisory. SSL virtual services on the Array appliances are not vulnerable to the specified attack as additional SSL hand shaking is required. Array Networks SSL layer will send an SSL alert to the attacker effectively resetting the connection immediately.