Array Networks Security Advisory for US CERT Vulnerability Note VU#261869

Date: - December 08, 2009

Overview

The security advisory is Array Networks response to US CERT Vulnerability Note VU#261869. Web Resource Mapping is a module that rewrites all URLs accessed through the Array SPX with the domain name of the access point. While access is typically meant for internal web sites, it is quite possible for external web sites to be accessed via the SSL VPN. Since all access is presented to the browser via the domain name of the SSL VPN, it is possible for an attacker to write some Javascript or other code that allows them to read browser's cookies and other information which are usually not available except for the domain that the user is interacting with. This could create a vulnerability that allows them to insert malicious code on the end-point which can cause a lot of damage.

Mitigation

There is no software fix for this attack since the function of URL rewrite is to provide such a mapping from all URLs accessed behind the gateway. Given the purpose of VPN is to provide access to internal resources; the damage can be mitigated by reducing or eliminating access to third-party resources. The Array SPX system provides many tools to reduce the security risk and bring it down to acceptable levels. Here are a few solutions:

1. Configure webwall rules or internal firewalls so that the SPX only accesses web sites and servers within the trusted domains.
2. Avoid providing access to external or risky URLs through the VPN. This can be accomplished by:
   a. Turn off user input bar for goto URLs: on the web portal
   b. Only configure links on the portal to have trusted applications or servers.
3. Where this is not possible, configure the list of TRUSTED sites as INTERNAL URLs and set the DEFAULT urlpolicy to be EXTERNAL. This will convert the rewrite to be a white list instead of black list. All untrusted URLs will be redirected without rewrite. The browser will only allow the server to read cookies for it, since it is no longer being proxied.
4. Disable URL Masking feature so that the user sees the interaction with the external web site via visible text in the URL bar, and is therefore more aware that they may be interacting with a site that they did not expect to interact with
5. Enable end-point security and have it check the host machine to make sure that approved anti-virus, anti-spam, anti-malware and personal firewall code is running on the end-point. Ensure cache cleaning is set to run and clean up the browser cache after the session is over.

6. Enable access from trusted end-points or hosts via Layer 3 VPN or DesktopDirect in to trusted INTERNAL domains, from which direct access is made to the resources.