Security Research Advisory – August 16, 2011

SAP J2EE engine compromised

What happened?

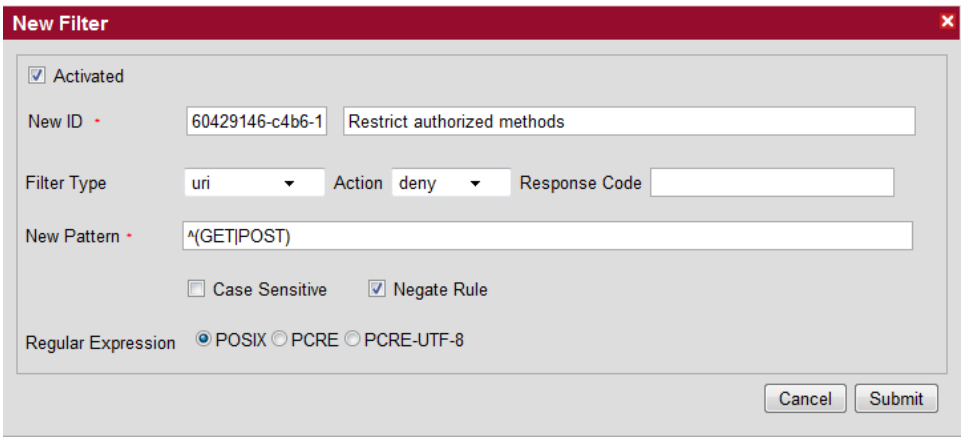
At the 2011 BlackHat conference, which was held in Las Vegas on August 3-4, Russian researcher Alexander Polyakov revealed a vulnerability in the J2EE engine of the SAP Netweaver portal. This vulnerability makes it possible for a remote attacker having access to the web interface of the portal, to create a user account and move it to the administrators groups. As a consequence any SAP Netweaver installation can be entirely compromised. SAP hasn't release a patch yet, leaving all the Netweaver platforms potentially exposed to an attack exploiting the vulnerability.

Attack description

The attack relies on a broken authentication mechanism which is applied only on explicitly named HTTP methods. While the common GET and POST methods are usually handled in the configuration file, this is rarely the case of the HEAD method. As a consequence, requests can be sent through this method, bypassing any authentication mechanism.

Mitigation

The DARC team recommends that all customers using rWeb and sProxy to protect SAP Netweaver environments create a specific Black List to ensure their applications are protected against a potential exploitation of this vulnerability. Version 4.0 of rWeb and sProxy make it easy to create a specific filter to block any method which would not be GET or POST, as shown below:



Moreover, Deny All's R&D team has made the decision to create an SAP Netweaver security policy profile, which will implement these restrictions by default, in the next Feature Pack of rWeb 4.0 and sProxy 4.0.

About the DARC

The Deny All Research Center (DARC) is an internal division of Deny All, which focuses on threat analysis and mitigation. Over the last 10 years, this department's research has contributed to the design of state-of-the art Web application security solutions. More information on Deny All can be found at www.denyall.com