Trustwave

Heartbleed Vulnerability Patch for Trustwave WAF v6.1 and 6.2

OpenSSL releases 1.0.1 through 1.0.1f have been found vulnerable to a security issue identified as **TLS Heartbeat Read Overrun** (CVE-2014-0160).

To address this vulnerability, Trustwave has issued a patch for WAF v6.1 and 6.2. The patch solves this critical security issue by upgrading Open SSL to version 1.0.1g. The patch will be included in all future software versions. WAF version 6.0 is also affected by the vulnerability. Customers running version 6.0 are advised to upgrade immediately and then apply the appropriate patch.

To obtain the patch, please contact WAF Support in the Trustwave TAC.

Please note that this patch will require a restart of the WAF services.

Deployment Considerations: The OpenSSL vulnerability for Trustwave WAF is only exploitable for inline deployment scenarios. If the Trustwave WAF is deployed out-of-line, any attack would be made against the web server, in which case exploitability depends on whether or not the web server itself is vulnerable. You can check for web server vulnerabilities via this open source tool: http://filippo.io/Heartbleed/

Full contact information for the Trustwave TAC WAF Support Services Team:

Email: WAFTACSupport@trustwave.com

Toll Free Phone: +1 (866) 659-9097, Option 3, 5
International Phone: 00 800 1954 1954, Option 3, 5
Support Portal: https://login.trustwave.com/
Knowledge Base: https://www.trustwave.com/support/kb/
For further questions and assistance, please contact Trustwave Support.