Xerox Security Bulletin XRX08-008

Software update to address Cross Site Scripting and SQL Injection vulnerabilities

v1.0
07/09/08

Background

As part of Xerox's continued focus on information security we periodically run industry security vulnerability software against out applications to ensure that they are not vulnerable to emerging security threats. Recently, our internal testing procedures uncovered vulnerabilities in the CentreWare Web (CWW) product. Three areas of the application are vulnerable to SQL Injection attacks, and two areas of the application are vulnerable to Cross Site Scripting attacks. If exploited, these vulnerabilities could allow an attacker to make unauthorized changes to CWW or asset data, or redirect user browsing sessions. Xerox is not aware of exploit code existing in the wild.

Mitigating controls exist for these vulnerabilities in the affected versions:

- Only authenticated CWW users can access the vulnerable areas of the application.

As part of Xerox's on-going efforts to protect customers, a software update is provided to remediate these issues. This solution is designed to be installed by the customer. Customers interested in upgrading to the newest version can download and install the update from the location below.

The patched version is 4.6.46, and can be downloaded with installation instructions from the following location:

http://www.support.xerox.com/go/results.asp?Xtype=download&prodID=CentreWare_Web&Xlang=en_US&Xcntry=USA

The rating for this release is **Moderate**.

Note: This update is version 4.6.46. Once the version is successfully installed, the application footer will reflect the new version.

The described vulnerabilities exist in the following CWW versions:

All versions of
CWW prior to
4.6.46