

XEROX SECURITY BULLETIN XRX06-001 ([This bulletin has been superseded by XRX06-003](#))

Vulnerabilities in the ESS/ Network Controller and MicroServer Web Server could potentially permit unauthorized access.

System Software Version 14.027.24.015 or 13.027.24.015, depending on whether the product is a WorkCentre® or WorkCentre® Pro, respectively, incorporates fixes for these vulnerabilities. A Xerox Customer Service Representative must install this software. To initiate the request for either of these software versions, please contact Xerox customer support and request the solution for Security Bulletin Number XRX06-001.

This software is Common Criteria validated and is listed on the National Information Assurance Partnership's Validated Products List at http://niap.nist.gov/cc-scheme/vpl/vpl_type.html.

Background

System Software Versions 13.027.24.015 and 14.027.24.015 has completed Common Criteria evaluation. The software applies to the products listed below.

This system software version incorporates fixes for vulnerabilities in the ESS/ Network Controller and MicroServer Web Server code that could allow unauthorized access including:

- Vulnerabilities that could bypass authentication or allow unauthorized network access.
- Specially constructed Postscript request can cause denial of service.
- Cross-site scripting allowing contents of web pages to be modified in an unauthorized manner.
- Vulnerabilities that could reduce effectiveness of some security features.

If successful, an attacker could make unauthorized changes to the system configuration. Customer and user passwords are not exposed.

Products Affected:

WorkCentre®	WorkCentre® Pro
232	232
238	238
245	245
255	255
265	265
275	275

Acknowledgments:

Xerox thanks the following for working with us to help protect our customers:

- Brendan O'Connor for reporting the cross-site scripting vulnerability

Disclaimer

The information in this Xerox Product Response is provided "as is" without warranty of any kind. Xerox Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this Xerox Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.