

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE ISSUED: July 21, 2015

SUBJECT: Vulnerability in Microsoft Font Driver Could Allow Arbitrary Code Execution in Windows Server 2003 (MS15-078)

An out-of-band patch was released for Microsoft Operating Systems that addressed a vulnerability in Microsoft Font Driver that could allow arbitrary code execution (CVE-2015-2426). The patch did not address Windows Server 2003 as it is no longer supported publicly by Microsoft, however, this vulnerability does affect Windows Server 2003.

Based on our current domain database, 9% of all Windows-based web servers are running Windows Server 2003.

RECOMMENDATIONS:

The following actions should be taken:

- Consider implementing the work around options outlined in Microsoft's bulletin listed in the references section below, taking into consideration that this option will result in reduced functionality for processing OpenType fonts.
- Consider procuring a custom support contract with Microsoft to continue supporting Windows Server 2003 instances that cannot be upgraded at this time.

REFERENCES:

<https://technet.microsoft.com/en-us/library/security/MS15-078>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>