

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(S) ISSUED:

09/13/2016

SUBJECT:

Security Update for Microsoft Exchange Server (MS16-108)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Exchange Server. Microsoft Exchange Server is an email server software product from Microsoft. The most severe of these vulnerabilities can result in remote code execution if an attacker sends an email with a specially crafted attachment to a vulnerable Exchange server. Successful exploitation could allow an attacker to gain the same privileges as a local server account. Depending on the privileges associated with the account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Microsoft Exchange Server the most severe of the which could allow remote code execution in some Oracle Outside In libraries that are built into

Exchange Server if an attacker sends an email with a specially crafted attachment to a vulnerable Exchange server. The vulnerabilities are as follows:

- Eleven Oracle Outside In Libraries vulnerabilities that could lead to remote code execution (CVE-2016-3575, CVE-2016-3581, CVE-2016-3582, CVE-2016-3583, CVE-2016-3595, CVE-2016-3594, CVE-2015-6014, CVE-2016-3593, CVE-2016-3592, CVE-2016-3596, CVE-2016-3591).
- An Oracle Outside In Libraries vulnerability that could lead to information disclosure (CVE-2016-3574).
- Six Oracle Outside In Libraries vulnerabilities that could lead to denial of service (CVE-2016-3576, CVE-2016-3577, CVE-2016-3578, CVE-2016-3579, CVE-2016-3580, CVE-2016-3590).
- An information disclosure vulnerability exists in the way Microsoft Exchange Server parses email messages (CVE-2016-0138).
- An open redirect vulnerability exists in Microsoft Exchange Server that could lead to spoofing (CVE-2016-3378).
- An elevation of privilege vulnerability exists in the way Microsoft Outlook handles meeting invitation requests (CVE-2016-3379).

The most severe of these vulnerabilities could allow an attacker to execute remote code. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms16-108.aspx>

CVE:

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6014>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0138>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3378>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3379>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3574>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3575>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3576>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3577>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3578>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3579>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3580>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3581>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3582>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3583>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3590>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3591>
<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3592>
<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3593>
<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3594>
<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3595>
<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3596>

TLP: WHITE

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

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