



# State of Alaska State Security Office

## State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

August 14, 2012

*The following cyber advisory was issued by the State of Alaska and was 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.*

### **MS-ISAC ADVISORY NUMBER:**

SA2012-048

### **DATE (S) ISSUED:**

08/14/2012

### **SUBJECT:**

Vulnerabilities in Microsoft Exchange Server WebReady Document Viewing Could Allow Remote Code Execution (MS12-058)

### **OVERVIEW:**

Multiple vulnerabilities have been reported in Microsoft Exchange Server WebReady Document Viewing that could allow remote code execution. Microsoft Exchange Server provides email, calendar and contacts for corporate environments. MS Exchange Server Web Ready Document viewing is a feature that allows Outlook Web Access (OWA) users to view attachments such as Microsoft Office documents within the browser.

Successful exploitation could allow an attacker to run arbitrary code within the context of the LocalService account on the affected Microsoft Exchange Server. Typically, the LocalService account has minimum privileges on the system.

### **SYSTEMS AFFECTED:**

- Microsoft Exchange Server 2007 SP 3
- Microsoft Exchange Server 2010 SP 1 & 2

### **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: N/A**

### **DESCRIPTION:**

Multiple vulnerabilities have been discovered in Microsoft Exchange Server WebReady Document Viewing that can allow an attacker to take complete control of a Windows Exchange Server. **Microsoft Exchange Server WebReady is enabled by default.**

This issue exists due to vulnerabilities contained within libraries of Oracle Outside In. These libraries are used when handling and rendering unstructured document formats. If disabled, OWA users may not be able to preview the content of email attachments.

To exploit this vulnerability, an attacker creates a specially crafted file that is sent via e-mail to a user on a vulnerable version of Microsoft Exchange Server. When the user opens the document within their browser, the attackers code runs within the privilege context of the LocalService account on the Microsoft Exchange Server. The LocalService account by default has limited system and file system privileges and sends only anonymous credentials over the network.

Successful exploitation could result in an attacker leveraging other vulnerabilities to escalate their privileges. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

#### **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems after testing.
- Evaluate the relative need for WebReady viewing and disable if deemed non-essential.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open un-trusted attachments from unknown or untrusted sources.

#### **REFERENCES:**

##### **Microsoft:**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-058>

##### **SecurityFocus:**

<http://www.securityfocus.com/54497>

<http://www.securityfocus.com/54511>

<http://www.securityfocus.com/54531>

<http://www.securityfocus.com/54536>

<http://www.securityfocus.com/54541>

<http://www.securityfocus.com/54543>

<http://www.securityfocus.com/54546>

<http://www.securityfocus.com/54548>

<http://www.securityfocus.com/54550>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1766>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1767>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1768>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1769>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1770>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1771>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1772>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1773>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3106>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3107>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3108>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3109>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3110>