



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

**July 12, 2016**

*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.*

**ADVISORY NUMBER:**

SA2016-100

**DATE(S) ISSUED:**

07/12/2016

**SUBJECT:**

Cumulative Security Update for Internet Explorer (MS16-084)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft Internet Explorer, the most severe of which could allow remote code execution if a user views a specially crafted webpage. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. 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.

**SYSTEMS AFFECTED:**

- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

**RISK:**

**Government:**

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

**Businesses:**

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

**Home users: Low**

## **TECHNICAL SUMMARY:**

- Multiple vulnerabilities have been discovered in Internet Explorer, the most severe of which could allow for remote code execution. The details of these vulnerabilities are as follows:
- Five Memory Corruption Vulnerabilities exist when Internet Explorer improperly accesses objects in memory (CVE-2016-3240, CVE-2016-3241, CVE-2016-3242, CVE-2016-3243, CVE-2016-3264)
- One restricted ports security feature bypass vulnerability (CVE-2016-3245)
- Four vulnerabilities in the way that JScript9 and VBScript engines render when handling objects in memory (CVE-2016-3204, CVE-2016-3248, CVE-2016-3259, CVE-2016-3260)
- Two information disclosure vulnerabilities due to improper handling of objects in memory (CVE-2016-3261, CVE-2016-3277)
- One information disclosure vulnerability exists when Microsoft Browser XSS Filter does not properly validate content under specific conditions (CVE-2016-3273)
- One spoofing vulnerability exists when a Microsoft Browser does not properly parse HTTP content (CVE-2016-3274)
- One spoofing vulnerability exists when a Microsoft Browser in reader mode does not properly parse HTML content (CVE-2016-3276)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute remote code by luring a victim to visit a specially crafted malicious website. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. Depending on the privileges associated with the user, an attacker could 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 immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the principle of Least Privilege to all systems and services.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

## **REFERENCES:**

### **Microsoft:**

<https://technet.microsoft.com/en-us/library/security/ms16-084.aspx>

### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3204>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3240>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3241>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3242>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3243>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3245>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3248>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3259>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3260>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3261>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3264>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3273>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3274>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3276>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3277>