

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.

DATE(S) ISSUED:

06/21/2012

SUBJECT:

Multiple Vulnerabilities in Cisco AnyConnect VPN Software Could Lead to Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco AnyConnect Virtual Private Network (VPN) client software that could allow for remote code execution. Cisco AnyConnect is VPN client software used to gain access to private networks. The application is prone to multiple vulnerabilities; some of which could result in remote code execution on the client. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. 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. Failed exploit attempts will likely cause denial-of-service conditions.

SYSTEMS AFFECTED:

- Cisco AnyConnect Secure Mobility Client VPN Downloader 2.x releases prior to 2.5 MR6 on MS Windows, Linux, and Mac OS
- Cisco AnyConnect Secure Mobility Client VPN Downloader 3.0.x releases prior to 3.0 MR8 on Linux, and Mac OS
- Cisco AnyConnect Secure Mobility Client 3.0.x releases prior to 3.0 MR8 on MS Windows, Linux, and Mac OS
- Cisco Secure Desktop Host Scan Downloader releases prior to 3.6.6020 on MS Windows, Linux, and Mac OS
- Cisco AnyConnect Secure Mobility Client 64-bit Java VPN Downloader 3.0.x releases prior to 3.0 MR7 on Linux 64-bit

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: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Cisco AnyConnect VPN client software that could allow for remote code execution. These vulnerabilities exist due to multiple errors in the Web Launch component, which is used to upgrade and/or install client software in a web-deployment scenario. Details of these vulnerabilities are as follows:

Cisco AnyConnect Secure Mobility Client VPN Downloader Arbitrary Code Execution Vulnerability:

Cisco AnyConnect Secure Mobility Client is prone to a remote code execution vulnerability due to input errors in the ActiveX and Java components that perform Web Launch functionality. To exploit this vulnerability, an attacker creates a specially crafted website and entices users to visit that site through e-mail or by some other means. Successful exploitation could occur if the user downloads the malicious ActiveX control or Java Applet. It should be noted that this may require additional user interaction depending on the user's browser settings. This vulnerability affects software versions 2.x releases prior to 2.5 MR6 on Microsoft Windows and Linux systems and 3.0.x releases prior to 3.0 MR8 on Apple MacOS systems (CVE-2012-2493)

Cisco AnyConnect Secure Mobility Client 64-bit Java VPN Downloader Arbitrary Code Execution Vulnerability:

Cisco AnyConnect Secure Mobility 64-bit Client is prone to a remote code execution vulnerability due to unspecified input errors in the Java Web Launch components. To exploit this vulnerability, an attacker must create a specially crafted website and entice users to visit that site through e-mail or by some other means. Successful exploitation could occur if the user downloads the malicious Java Applet. It should be noted that this may require additional user interaction depending on the user's browser settings. This vulnerability affects software versions 3.0.x releases prior to 3.0 MR7 on Linux 64-Bit systems. (CVE-2012-2496)

Cisco AnyConnect Secure Mobility Client VPN Downloader Software Downgrade Vulnerability:

Cisco AnyConnect Secure Mobility Client contains multiple remote downgrade vulnerabilities due to input errors in the ActiveX and Java components that perform the Web Launch functionality. To exploit this vulnerability, an attacker must create a specially crafted website and entice users to visit the site through e-mail or by some other means. Successful exploitation could occur if the user downloads a malicious ActiveX control or Java Applet and may result in the client software being downgraded to a previous version. This could require additional user interaction depending on the user's browser settings. These vulnerabilities affect the following software releases: 2.x releases prior to 2.5 MR6 and 3.0.x releases prior to 3.0 MR8 on Microsoft Windows, Linux, and Apple MacOS X (CVE-2012-2494). 3.0.x releases prior to 3.0 MR8 on Microsoft Windows, Linux, and MacOS X (CVE-2012-2495) are also affected.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Cisco after appropriate testing. To view a complete list of what software fixes to apply, please see <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ac#@ID>
- Consider implementing the workaround provided by Cisco which prevents the vulnerable code from initiating. To view the instructions for this workaround please see <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ac>
- Configure Internet Explorer to prompt before running Active Scripting or disable Active Scripting to temporarily mitigate this vulnerability.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:**Cisco:**

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-ac#@ID>

Security Focus:

<http://www.securityfocus.com/bid/54107>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2493>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2494>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2495>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2496>