



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

August 26, 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:

SA2016-124

DATE(S) ISSUED:

08/25/2016

SUBJECT:

Multiple Vulnerabilities in Apple Products Could Allow For Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in iOS, the most severe of which could allow for arbitrary code execution. Apple iOS is an operating system for iPhone, iPod touch, and iPad. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code with kernel privileges.

THREAT INTELLIGENCE:

These vulnerabilities are associated with three zero-days (nicknamed "Trident") and a tool called "Pegasus." These vulnerabilities have been publicly disclosed and a tool exists to perform the exploit. There are reports of the vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- iOS prior to 9.3.5 for iPhone 4s and later, iPod touch (5th generation) and later, and iPad 2 and later

RISK:

Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:

Apple has released patches for multiple vulnerabilities that have been discovered in Apple products. These vulnerabilities can be exploited by convincing a user to visit a specially crafted webpage. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A vulnerability exists in the kernel that may lead to disclosure of the kernel's location in memory (CVE-2016-4655).
- A vulnerability exists in the kernel that may lead to memory corruption and covert jailbreaking of the device (CVE-2016-4656).
- A vulnerability exists in Webkit, allowing for memory corruption (CVE-2016-4657).

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by [Apple](#) to vulnerable systems immediately after appropriate testing.
- 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:

Apple:

<https://support.apple.com/en-us/HT207107>

Lookout:

<https://blog.lookout.com/blog/2016/08/25/trident-pegasus/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4655>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4656>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4657>

· Bug #72564 (boolean always deserialized as "true") (Remi)

· Bug #72142 (WDDX Packet Injection Vulnerability in wddx_serialize_value()).

· Bug #72749 (wddx_deserialize allows illegal memory access) (Stas)

· Bug #72750 (wddx_deserialize null dereference).

- Bug #72790 (wddx_deserialize null dereference with invalid xml).
- Bug #72799 (wddx_deserialize null dereference in php_wddx_pop_element).
- Bug #72660 (NULL Pointer dereference in zend_virtual_cwd).

Successful exploits may allow an attacker to inject and run arbitrary code in the context of the application or obtain sensitive information that may aid in further attacks. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade to the latest version of PHP immediately, after appropriate testing.
- Apply the principle of Least Privilege to all systems and services.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to only those required.

REFERENCES:

NOTE: Visiting these links may trigger an IDS signature match for a Possible Encrypted Webshell Download. This is a false positive alert that is matching content on the pages below.

PHP:

<http://php.net/ChangeLog-7.php>

<http://php.net/ChangeLog-5.php>