



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

November 15, 2013

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:
SA2013-093

DATE ISSUED: 11/15/2013

SUBJECT: ColdFusion Backdoor on Government Websites

The MS-ISAC has received information from a trusted third party indicating that cyber hackers associated with Anonymous used a zero-day authentication bypass vulnerability in Adobe ColdFusion to compromise U.S. Government web servers. This vulnerability allowed the attackers to interact with the victim Web server's administrative panel without the administrative password by targeting "\CFIDE\adminapi\administrator.cfc." The Adobe ColdFusion vulnerability was identified by Adobe as APSB13-03 and was patched on January 15, 2013 and is associated with the following CVE numbers:

- CVE-2013-0625
- CVE-2013-0629
- CVE-2013-0631
- CVE-2013-0632

Upon exploitation of this vulnerability, the hackers installed backdoors on the exploited systems to assure future access and to exfiltrate data from the compromised systems. The backdoor files utilized the password "trip1337DAY." The backdoors that were dropped onto the systems are associated with the following files:

- h.cfm (MD5 hash value: e7ae3fd87da7e473a897ccf19f3eda0a)
- i.cfm (MD5 hash value: e7ae3fd87da7e473a897ccf19f3eda0a)
- r.cfm
- sq.cfm (MD5 hash value: 0a938e6197f89d3b0d07976a69c4caaf)
- header2.cfm
- lastresort.cfm
- olr.7z

- help.cfm
- h9.cfm
- konami.js
- mappings.cfm (MD5 hash value: 2fa19dad40115be50e8f81625bef04b8)
- mappings1.cfm (MD5 hash value: 75c8183c9718cb9cac003545a7e51a3f)
- mappings2.cfm (MD5 hash value: 2fa19dad40115be50e8f81625bef04b8)
- mappings3.cfm (MD5 hash value: 75c8183c9718cb9cac003545a7e51a3f)
- probe.cfm (MD5 hash value: 81083a956264d87834ec0daea3e93d1f)
- scheduleedit.cfm (MD5 hash value: 0c54d4792e58c1ab40b28c15c2395a95)
- scheduleedit1.cfm (MD5 hash value: 2122f96bf1f6424a522343d815e163b3)
- scheduleedit2.cfm (MD5 hash value: 2122f96bf1f6424a522343d815e163b3)
- scheduletasks.cfm (MD5 hash value: e04c6fc5a4571fb2b51a3fa8d03099e0)
- scheduletask1.cfm (MD5 hash value: 82df6de1e45868c437a8a3d1a4abe169)
- scheduletask2.cfm (MD5 hash value: 82df6de1e45868c437a8a3d1a4abe169)
- CFUP1934.cfm (MD5 hash value: 2f151c0f02952d3983ecac15532da997)
- CFUP4321.cfm (MD5 hash value: 2f151c0f02952d3983ecac15532da997)
- CFUP6939.cfm (MD5 hash value: 2f151c0f02952d3983ecac15532da997)
- CFUP9413.cfm (MD5 hash value: 2f151c0f02952d3983ecac15532da997)
- Index.cfm (MD5 hash value: 6b025d644d40a1f61503c0052677d97c)
- Plan2.cfm (MD5 hash value: b42a5b07fba7e4af0aeea80977536f5d)
- Plan21.cfm (MD5 hash value: b42a5b07fba7e4af0aeea80977536f5d)
- Plan27.cfm (MD5 hash value: b42a5b07fba7e4af0aeea80977536f5d)
- Plan37.cfm (MD5 hash value: b42a5b07fba7e4af0aeea80977536f5d)
- Plan58.cfm (MD5 hash value: b42a5b07fba7e4af0aeea80977536f5d)
- Trip.jar (MD5 hash value: 787370cf679812b576a8b83ec99b1612)

According to the source of the information, the initial compromises started in December 2012 and were a part of the Anonymous campaign "Operation Last Resort". Currently, it is unknown how many systems are affected by this issue.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Ensure that none of the potentially malicious files listed above are on your server.
- If the backdoors are identified, notify MS-ISAC immediately for further assistance
- Ensure that servers running Adobe ColdFusion are up to date.