



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

August 29, 2014

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:

SA2014-054

DATE(S) ISSUED:

08/29/14

SUBJECT:

Vulnerability in Multiple F5 products could allow for Remote code execution.

EXECUTIVE SUMMARY:

A vulnerability has been discovered in multiple F5 Big IP and Enterprise Manager products which could allow for remote code execution. F5 provide multiple security products, such as firewalls and web gateways.

Successful exploitation of this vulnerability could result in an attacker gaining root access to the affected devices. An attacker would then have full read/write access.

THREAT INTELLIGENCE

There is proof-of-concept code is publically available.

SYSTEM AFFECTED:

- F5 BIG-IP LTM 11.0.0-11.5.1
- F5 BIG-IP AAM 11.4.0 - 11.5.1
- F5 BIG-IP AFM 11.3.0 - 11.5.1
- F5 BIG-IP Analytics 11.0.0 - 11.5.1
- F5 BIG-IP APM 11.0.0 - 11.5.1
- F5 BIG-IP ASM 11.0.0 - 11.5.1
- F5 BIG-IP Edge Gateway 11.0.0 - 11.3.0
- F5 BIG-IP GTM 11.0.0 - 11.5.1
- F5 BIG-IP Link Controller 11.0.0 - 11.5.1
- F5 BIG-IP PEM 11.3.0 - 11.5.1
- F5 BIG-IP PSM 11.0.0 - 11.4.1
- F5 BIG-IP WebAccelerator 11.0.0 - 11.3.0
- F5 BIG-IP WOM 11.0.0 - 11.3.0
- F5 Enterprise Manager 3.0.0 - 3.1.1

RISK:

Government:

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

Businesses:

- Large and medium business entities: High
- Small business entities: Low

Home users: Low

TECHNICAL SUMMARY:

A remote code execution vulnerability has been discovered in multiple F5 BIG-IP products which can allow remote unauthorized root access to affected devices. Specifically when configured in a high availability/failover mode, the devices suffer from an unauthenticated rsync access vulnerability. Rsync is program used to ensure that files and directories on two different systems are the same. The rsync daemon does not require authentication when communicating to a ConfigSync IP. An attacker could upload a malicious SSH key to the root folder directly and create a SSH session on the device.

- ConfigSync-IP Rsync full file system access vulnerability [CVE-2014-2927]

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade vulnerable F5 products immediately after appropriate testing.
- Set the ConfigSync self IP's port lockdown setting to not allow all and limit TCP port 873 access.
- Filter access to the affected device at the network boundary if global access isn't needed. Restricting access to only trusted computers and networks might greatly reduce the likelihood of a successful exploit.

REFERENCES:

F5:

<http://support.f5.com/kb/en-us/solutions/public/15000/200/sol15236.html>

Security-Assessment:

http://www.security-assessment.com/files/documents/advisory/F5_Unauthenticated_rsync_access_to_Remote_Root_Code_Execution.pdf

Security Focus:

<http://www.securityfocus.com/bid/69461>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2927>