

*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:**

6/12/2012

**SUBJECT:**

A Vulnerability in Multiple F5 Products Could Allow Unauthorized Access

**OVERVIEW:**

A vulnerability has been discovered in multiple F5 BIG-IP based products which could allow remote unauthorized access to an affected device. BIG-IP is a network appliance developed by F5. A remote attacker can exploit this issue to gain unauthorized root access to affected devices. Successfully exploiting this issue allows an attacker to completely compromise the device.

**SYSTEMS AFFECTED:**

- BIG-IP prior to 9.4.8-HF5
- BIG-IP prior to 10.2.4
- BIG-IP prior to 11.0.0-HF2
- BIG-IP prior to 11.1.0-HF3
- Enterprise Manager prior to 2.1.0-HF2
- Enterprise Manager prior to 2.3.0-HF3

**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:** N/A

**DESCRIPTION:**

An SSH configuration vulnerability has been discovered in multiple F5 BIG-IP products which can allow remote unauthorized root access to affected devices. Specifically, this issue occurs because the SSH private key corresponding to the public key used by these affected devices is present on all BIG-IP appliances and is publicly available. Successful exploitation allows attackers to completely compromise the device.

**RECOMMENDATIONS:**

The following actions should be taken:

- Upgrade vulnerable F5 products immediately after appropriate testing. If you are unable to apply the update immediately, consider applying the work-around issued by F5 which reconfigures the SSH access to the device.
- Expose the management interface only on trusted networks.
- 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/13000/600/sol13600.html>

**Trust Matta:**

<https://www.trustmatta.com/advisories/MATTA-2012-002.txt>

**SecurityFocus:**

<http://www.securityfocus.com/bid/53897>