



UX WORLD, INC.

dnsfly Appliance for AWS

Version 4.1.3

Release Notes

UX WORLD, INC.

COPYRIGHT

Copyright (c) 2005-2012 UX WORLD, INC. All rights reserved.

The product and documentation are subject to change without notice.

PROPRIETARY NOTICES

“UX WORLD” and “*dnshly*” are the trademarks of UX WORLD, INC.

“Amazon AWS”, “Amazon EC2” and “Amazon Elastic Cloud Compute” are service or trade marks of Amazon Web Services LLC.

Version 4.1.3

Introduction

dnsfly version 4.1.3 is released to address the “shell shock” security vulnerability. This release addresses following vulnerabilities on the base Red Hat Linux distribution:

1. CVE-2014-6271: Arbitrary code execution
2. CVE-2014-7169: Specially crafted environment variables containing arbitrary commands can be executed.

Further details on the vulnerability and diagnostic details are available at:

<https://access.redhat.com/solutions/1207723>

Deployment

dnsfly can be deployed from your AWS console. Please refer to the [*dnsfly Virtual Appliance for AWS – Initial Configuration Guide*](#) for further details:

Initial Admin Password

dnsfly's initial admin password is the instance ID. This password would be forced to change during the initial setup after the launch. The password may be reset to the instance-id or a new one from the recovery menu.

Updating existing instances

An existing instance may be patched by following steps:

1. ssh to your instance as *dnsflyadm*
2. Exit to the shell prompt
3. Run *yum update* command and follow the prompts:

```
$ sudo yum update bash
```