

Honeywell Security
2 Corporate Center Drive
Suite 100
Melville, NY 11747

October 3, 2014

IMPORTANT NOTICE – BASH VULNERABILITY

Bash is a very common software component embedded in products that utilize UNIX or Linux. Like many companies, Honeywell uses it in some of our products.

The security of our products is important to our customers and a priority for Honeywell. Our teams are working on this issue as quickly as possible to determine which of our connected products could be affected.

This software component could have security vulnerabilities and Honeywell is working to determine the extent of products that have this vulnerability. Honeywell has hundreds of connected products, and we expect that a small percentage may be affected by this vulnerability. For those Honeywell products that are affected by the vulnerability, we will develop a downloadable security patch to correct the issue and notify our customers when it's ready. To date we've determined the following products contain a vulnerable version of Bash:

- Tuxedo
- VAM
- NetAXS-4

However, it's important to note that because a product contains a vulnerable version of Bash does not mean that the product can be compromised. We are diligently reviewing each of these products to determine whether the Bash vulnerability can be exploited.

In the meantime, customers can take a few practical steps to protect their network from this issue:

- If possible, create additional layers of defense to their system from the Internet by placing the affected hardware behind a firewall and ensuring that port forwarding to the device is turned off.
- If remote connections to the device are required consider installing a VPN to ensure secure remote connections into the network the device is on.

Products such as Tuxedo and VAM initiate their connections to the AlarmNet network. Placing these devices behind firewalls at customer locations will have no impact to the ability of the device to function with the AlarmNet service.

As Honeywell makes a final determination and/or fix to this issue we will communicate this to our customers when it is available.