naked security by SOPHOS

SOPHOS.COM › FREE TOOLS ›

Award-winning computer security news

Industrial gas detectors vulnerable to a remote ‘attacker with low skill’

Security threats, Vulnerability
07 DEC 2015

by Mark Stockley

Users of Honeywell's Midas and Midas Black gas detectors are being urged to patch their firmware to protect against a pair of critical, remotely exploitable vulnerabilities.

These extremely serious vulnerabilities, found by researcher Maxim Rupp and reported by ICS-CERT (the Industrial Control Systems Cyber Emergency Response Team) in advisory ICSA-15-309-02, are simple enough to be exploited by an "attacker with low skill":

> *Successful exploitation of these vulnerabilities could allow a remote attacker to gain unauthenticated access to the device, potentially allowing configuration changes, as well as the initiation of calibration or test processes.*
>
> *…These vulnerabilities could be exploited remotely.*
>
> *…An attacker with low skill would be able to exploit these vulnerabilities.*

The affected devices are the Midas product with all firmware versions up to and including version 1.13b1 and the Midas Black product with all firmware versions up to and including version 2.13b1.

Patches are available to download from Honeywell's website under the banner of Honeywell's Security Notification SN 2015-10-14 01.

Midas and Midas Black gas detectors are used worldwide in numerous industrial sectors including chemical, manufacturing, energy, food, agriculture and water to:

> *...detect many key toxic, ambient and flammable gases in a plant. The device monitors points up to 100 feet (30 meters) away while using patented technology to regulate flow rates and ensure error-free gas detection.*

The vulnerabilities could allow the devices' authentication to be bypassed completely by path traversal (CVE-2015-7907) or to be compromised by attackers grabbing an administrator's password as it's transmitted in clear text (CVE-2015-7908).

In other words, the devices affected might be sophisticated and highly specialised but their bugs aren't. These are basic, workaday flaws that are well understood, easy to avoid and easy to test for.

It's shocking that such basic flaws should be present in software with such an important job to do but they wouldn't be nearly so serious if they weren't remotely exploitable.

Because these devices can be connected to the internet, the people they protect are at risk from anyone who can find a connected device (and if you're wondering if that's difficult, remember that the Internet of Things has its own search engine).

But perhaps we shouldn't be surprised because in many ways that's the story of the Internet of Things so far – a collection of interconnected devices from the future exhibiting vulnerabilities from the past.

The rush to attach kettles, TVs and baby monitors to the internet in the hope that it might be useful flies in the face of that bastion of security common sense; the principle of least privilege and it seems to me that it isn't going all that well so far.

The advisory offers the following pointers for minimising the risk of these flaws being exploited, although I suggest we'd all do well to follow them no matter if we're running industrial control systems or overly-clever thermostats:

- Minimise devices' network exposure and physical access
- Isolate devices from the internet and business networks
- Put devices behind a firewall and connect over a VPN if you need remote access

Or, put another way, treat the Things in the Internet of Things like computers, because they are.

Follow @NakedSecurity 41.8K followers

Follow @MarkStockley 463 followers

Image of Gas Mask courtesy of Shutterstock.

CVE-2015-7907 CVE-2015-7908 Gas Detectors Honeywell ICSA-15-309-02 internet of things iot SN 2015-10-14 01 vulnerability

Free tools

Sophos Home Beta

XG Firewall Home Edition

Mobile Security for Android

Virus Removal Tool

Antivirus for Linux

Antivirus for Mac

Previous: Monday revi...

Next: Has Mark Zucker...

About the author

Mark Stockley ▸

Mark Stockley is an independent web consultant who's interested in literally anything that makes websites better. Follow him on Twitter at @MarkStockley

Leave a Reply

Enter your comment here...

Recommended reads

AUG
13 BY PAUL DUCKLIN

Apple issues updates for lots of critical holes – patch now!

MAY
05 BY PAUL DUCKLIN

Bugs in the hospital: how to pwn your own pethidine machine

SOPHOS

About Naked Security
Our Authors
Send us a tip
About Sophos
Free Tools

NETWORK PROTECTION

XG Firewall
UTM
Secure Wi-Fi
Secure Web Gateway
Secure Email Gateway

ENDUSER PROTECTION

Enduser Protection Bundles
Endpoint Antivirus
Sophos Cloud
Mobile Control
SafeGuard Encryption

SERVER PROTECTION

Virtualization Security
Server Security
SharePoint Security
Network Storage
Antivirus
PureMessage

Powered by WordPress.com VIP