Honeywell

Security Notification
SN 2021-07-29

29 July 2021

PHD INSECURE PASSWORD ENCRYPTION STORAGE

This article contains:

- Summary
- Potential Vulnerability Synopsis
- Affected Products
- Resolution Description
- Appendix: About CVSS

To mitigate the risk:

- Follow Resolution Description procedure.

It applies to:

"Affected Products and Versions" section of this notice

Summary

This security notification addresses an issue reported on insecure password storage in Honeywell PHD.

Honeywell PHD (version R400 and earlier) stores PHD Service account credentials in the registry using an insecure encryption mechanism. The PHD server account password may be decrypted by a user with sufficient rights, by logging on to the PHD server.

Vulnerability Synopsis

Honeywell PHD (through version R400 inclusive) stores PHD service account credentials in the registry using an encryption key that is dynamically generated from known inputs. The passwords for these PHD service accounts may be decrypted by a user who has been provided with the elevated rights, due to the weak encryption methodology.

Local access to an affected PHD server by a non-privileged user is required to extract PHD service account passwords

CVSS Base Score: 7.8 (High)
CVSS Vector: CVSS:3.0/AV: L/AC: L/PR: L/UI: N/S: U/C:H/I:H/A:H

Affected Products and Versions

The potential vulnerability affects the following product versions: PHD400 and earlier versions of PHD.

Mitigating Factors

Honeywell recommends the following:

- Follow the PHD guidelines for the PHD service account in the domain.
- Both Test and Production servers should be configured correctly to limit the access to those accounts that require Admin rights as per Server Guidelines.
- The current PHD Service Account Password should be changed.
- The customer should be encouraged to upgrade to PHD R410.
- Under no circumstances give the PHD service account more rights than required (PHD guidelines) i.e. this account should not have system wide privileges.

PDF
PHD Security and
Network Planning Gu

PDF
PHD Security
Administration User G

Resolution Description

- In PHDR410 the password has been encrypted using common encryption best practices and is unique to each system.
- If using any version of PHD prior to R410, secure the domain and PHD service accounts as per the PHD guidelines above.

Acknowledgments

This was observed by providing the user with PHD server logon and making the user a member of the PHD product administrator group. In addition, the user was provided sufficient privileges to change the PHD service account password, run registry edit and run PowerShell on the PHD Server.

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS but is not supplied as it will differ for each customer.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES “AS IS” WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.