Honeywell

Security Notification
SN 2019-10-25 01

25 Oct 2019

Unauthenticated RCE via unsafe binary deserialization

Unauthenticated Remote arbitrary SQL command execution

This article contains:

It applies to:

MAXPRO VMS/NVR products listed in the “Affected Products” section of this notice

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

Knowledge of MAXPRO VMS/NVR system

Ability to use common Windows Tools

Skilled Hacker/Researcher

Summary

This security notification informs users of Honeywell MAXPRO VMS of an identified potential security vulnerability. Honeywell recommends users to follow the process described in the “Mitigating Factors” section to ensure this potential vulnerability is mitigated in any installed and operational system.

Attention: Due to the wide variety of security controls, implementations and interfaces, it is the responsibility of each customer to assess the potential impact within a specific operating environment.

Vulnerability Synopsis

MAXPRO Server have two potential vulnerability in Unauthenticated RCE via unsafe binary deserialization, Unauthenticated Remote arbitrary SQL command execution.

CVSS Base Score: 8.1 (High)

Temporal Score: 7.3 (High)

CVSS Vector
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Affected Products

The potential vulnerability affects the following product versions:

MAXPRO VMS	MAXPRO NVR
• **HNMSWVMS** • **HNMSWVMSLT**	• MAXPRO NVR XE • MAXPRO NVR SE • MAXPRO NVR PE • MPNVRSWXX

The updated patch for the above products is available for download on Mywebtech. We strongly recommend you download and install the latest updates.

Download Center > MAXPRO VMS > MAXPRO VMS R560 > MAXPRO VMS 560 Build 595 T2-Patch

Download Center > MAXPRO NVR > MAXPRO NVR 5.6 > MAXPRO NVR 5.6 Build 595 T2-Patch

Mitigating Factors

Honeywell recommends that customers with potentially affected products take the following steps to protect themselves:

- Update MAXPRO VMS and NVR to latest R560 and 5.6 before applying this patch
- Update software patch as per this security notification;
- As a best practice, we recommend Isolate your system from the Internet or create additional layers of defense to their system from the Internet by placing the affected hardware behind a firewall or into a DMZ; and
- If remote connections to the network are required, consider using a VPN or other means to ensure secure remote connections into the network where the device is located.

Resolution Description

Honeywell has released updated packages for all affected products listed above.

The package can be downloaded from:

https://mywebtech.honeywell.com/Home

Attention: This update should be installed by qualified personnel. Access credentials are required to access this site.

Contacting Support

For help installing, operating, maintaining, and troubleshooting this product, refer to this document and any other documentation provided. If you still have questions, contact us during business hours (Monday through Friday, excluding holidays).

Notes: Please be ready at the equipment before calling.

Table 1: Technical support

North America
T +1 800 323 4576
W **www.security.honeywell.com/**
Middle East, Turkey & Africa
T +9 714 454 1704
W **www.security.honeywell.com/me**
Europe
T +44 (0) 1928 754 028
W **www.security.honeywell.com/uk**
Asia Pacific
T +400 840 2233
W **www.security.honeywell.com/**

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 Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

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.

Honeywell would like to acknowledge Joachim Kerschbaumer for bringing this vulnerability to our attention via Honeywell PSIRT