Honeywell

Security Notification
SN 2024-06-25 01

25 June 2024

MAXPRO NVR Computer: Intel® Chipset Device Software - Uncontrolled Search Path Element

This article contains:

It applies to:

Maxpro NVR computer with Intel® Chipset Device Software before version 10.1.19444.8378

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

Qualified personnel with Maxpro Admin credentials

Summary

This security notification informs users of MAXPRO® SE NVR Rev D and XE NVR Rev D of the vulnerability that has been identified in the Intel® Chipset Device Software. Honeywell recommends that immediate steps be taken 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.

Potential Vulnerability Synopsis

1. [CVE-2023-28388]

   Description: Uncontrolled search path element in some Intel® Chipset Device Software before version 10.1.19444.8378 may allow an authenticated user to potentially enable escalation of privilege via local access.

   CVSS Base Score: [6.7] (Medium)

   CVSS Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

Affected Products

The potential vulnerability affects the following product versions:

- MAXPRO® SE NVR Rev D and XE NVR Rev D with Intel® Chipset Device Software before version 10.1.19444.8378.

Mitigating Factors

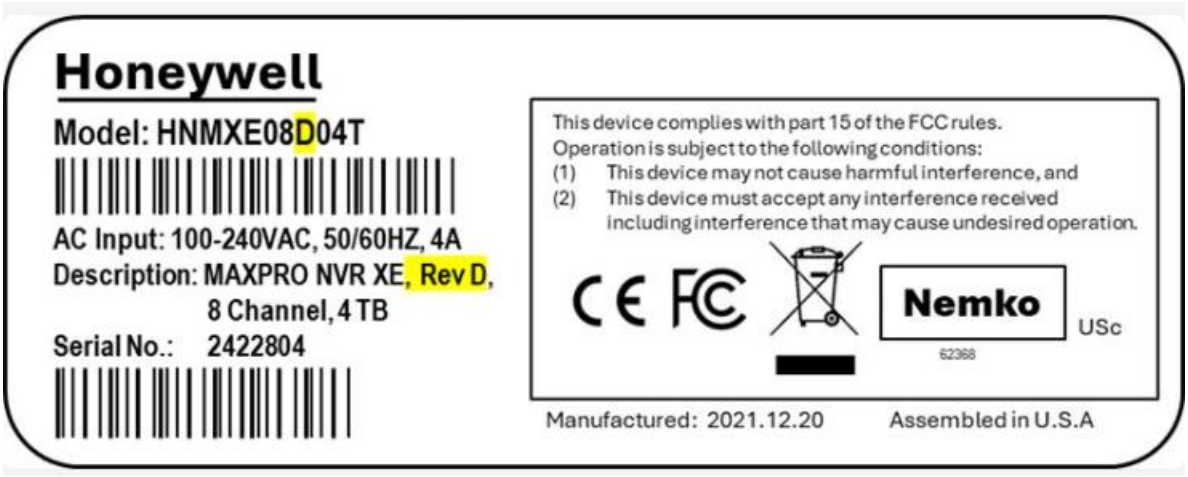
Honeywell recommends that customers with affected products should take the following steps to protect themselves:

- Check the Intel® Chipset Device Software version.
- If the version is earlier than 10.1.19444.8378, update the software.

Resolution Description

[How to check the NVR model revision]

Step 1. Locate the white asset tag on NVR unit (usually in back of the unit). Example asset tag is provided below as reference:



Step 2. The revision of the model is noted in the Model number/SKU and is the alpha-character in the position highlighted in yellow in the image above. It is also noted in the Description as highlighted above. If it is a “D” or “Rev D” then proceed with next section “How to check the Intel® Chipset Device Software”

[How to check the Intel® Chipset Device Software]

Step 1. Click Start

Step 2. Search and click Add/Remove Programs

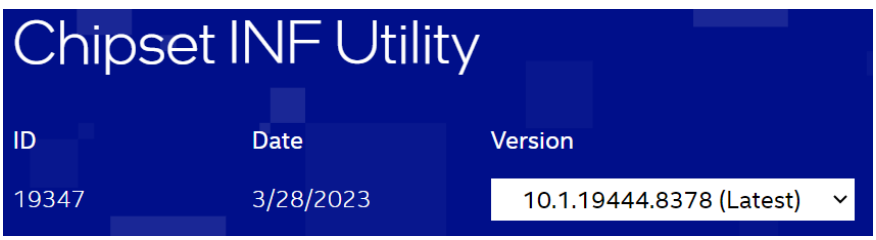
Step 3. Locate and click Intel(R) Chipset Device Software.

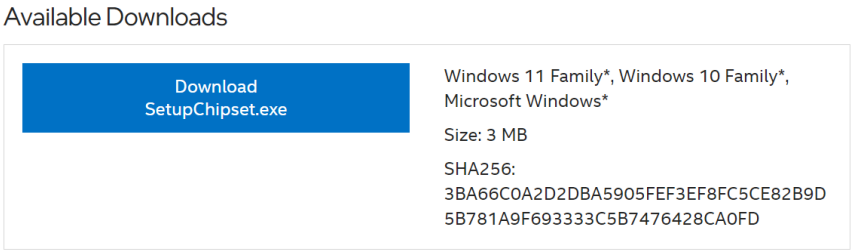
[How to update the Intel® Chipset Device Software]

Step 1. Go to Intel chipset INF utility at below link.

https://www.intel.com/content/www/us/en/download/19347/chipset-inf-utility.html

Step 2. Download 10.1.19444.8378



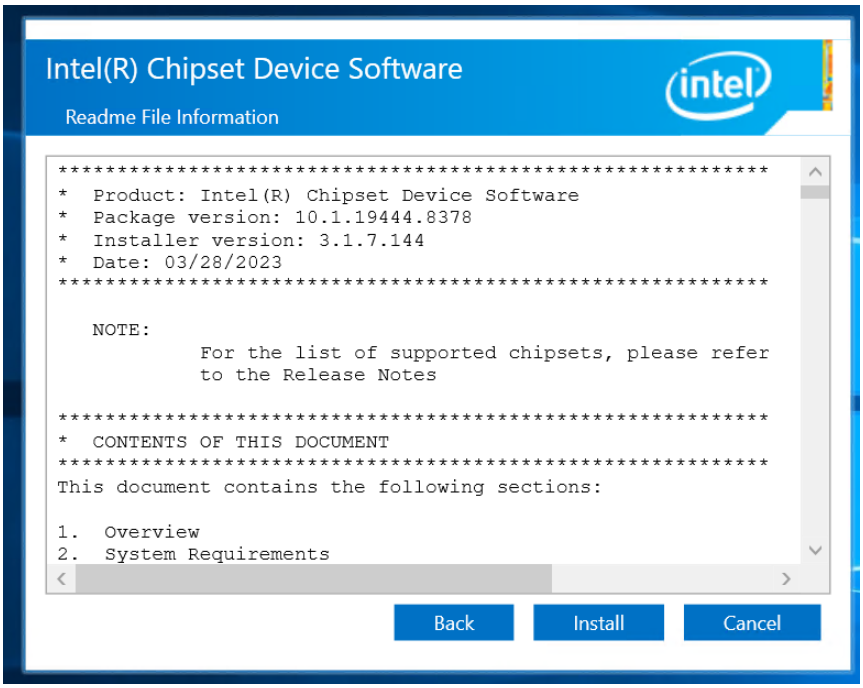


Step 3. Click on “Setup Chipset”

Step 4. Select Next

Step 5. Accept License Agreement

Step 6. Select “Install” to install the driver.



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.