Minimum Security Revision Control for Intel® Ethernet Products

Application Note

Ethernet Products Group (EPG)

July 2021

Revision 1.1
635205-002

Revision History

Revision	Date	Comments
1.1	July 16, 2021	Updated include the following: • Updated Section 4.1, "View Your Device's Current SRev and MinSRev".
1.0	February 9, 2021	Initial public release.

Did this document help answer your questions?

👍 👎

1.0 Introduction

This document addresses Minimum Security Revision control for products based on the following Intel devices:

- Intel® Ethernet Controller E810 (E810)
- Intel® Ethernet Controller X710/XXV710/XL710 (X710/XXV710/XL710)
- Intel® Ethernet Controller X710-TM4/AT2 (X710-TM4/AT2)
- Intel® Ethernet Controller X550 (X550)
- Intel® Ethernet Connection X722 (X722)

For more detailed information on supported features for each of these devices, see the following:

Device	Document	Doc ID
E810	Intel® Ethernet Controller E810 Feature Support Matrix	630155
X710/XXV710/XL710	Intel® Ethernet Controller X710/XXV710/XL710 Feature Support Matrix	332191
X710-TM4/AT2	Intel® Ethernet Controller X710-TM4/AT2 and V710-AT2 Feature Support Matrix	619407
X550	Intel® Ethernet Controller X550 Feature Support Matrix	335253
X722	Intel® Ethernet Connection X722 Feature Support Matrix	336882

2.0 Security Updates

Intel or your equipment manufacturer occasionally releases firmware security patches as part of a NVM release. The NVM contains the firmware and other critical components for the device operation. Intel recommends that you update your firmware to the latest version available for your device to take advantage of these security patches. Firmware updates for Intel Ethernet devices have a Security Revision number (SRev). The SRev might be updated as part this NVM release.

For the latest security information on Intel products, go to the Intel Security Center at:

https://www.intel.com/content/www/us/en/security-center/default.html

3.0 Minimum Security Revision Enforcement

Firmware updates can include security related updates. Downgrades of firmware can re-expose security issues. If you install a previous version of the NVM onto your device, security updates in the later version are not applied. Intel NVM releases include a Minimum Security Revision (MinSRev) enforcement feature. The MinSRev is lowest SRev the device allows to be installed and by default is preserved on NVM update. This mechanism is applied no matter the method used for NVM Update. This includes using the **nvmupdate** tool and when supported, FMP and PLDM firmware update. The NVM update process blocks the update if the supplied NVM has a lower SRev than the MinSRev value of the NVM currently loaded on the device.

When using the **nvmupdate** tool, you can update the MinSRev value during the firmware update process, locking the current security version in as the new MinSRev baseline, by using the -**optinminsrev** command line option. Only update the MinSRev value if you are certain you will not need to roll the firmware back to an earlier version. This means you can block the installation of a lower revision of the firmware onto your device. However, this limits the rollback capabilities of your device once this is done.

Caution: Once the MinSRev is increased, this is irreversible. NVM downgrades attempting to install a lower SRev than the current MinSRev will be rejected by the device. Although not recommended, leaving the MinSRev field unmodified allows firmware downgrades from any version to any version.

4.0 Examples

4.1 View Your Device's Current SRev and MinSRev

You can use the **nvmupdate** tool's inventory mode to view your device's current SRev and MinSRev values, as follows:

On Windows:

```
nvmupdatew64e -i -optinminsrev -l update.log -o update.xml -c nvmupdate.cfg
```

On Linux:

```
nvmupdate64e -i -optinminsrev -l update.log -o update.xml -c nvmupdate.cfg
```

Where:

`-i` — Sets **nvmupdate** to inventory mode.

`-optinminsrev` — In inventory mode this tells the tool to display the MinSRev value without updating it.

`-l update.log` — Specifies the name of the log file.

`-o update.xml` — Specifies the name of the results file. This is an XML file that contains the inventory/update results.

`-c nvmupdate.cfg` — Specifies the name of the configuration file. This is a text file that contains descriptions of networking devices and firmware versions for those devices.

Examine the *update.xml* file for the SRev and MinSRev values.

4.2 Update Your Device's MinSRev

Download and extract the NVM Update Package for your device. Use the command line to update your device's MinSRev:

On Windows:

```
nvmupdatew64e -u -optinminsrev -l update.log -o update.xml -c nvmupdate.cfg
```

On Linux:

```
nvmupdate64e -u -optinminsrev -l update.log -o update.xml -c nvmupdate.cfg
```

Where:

`-u` — Sets **nvmupdate** to update mode.

`-optinminsrev` — Tells the tool to update the MinSRev value.

`-l update.log` — Specifies the name of the log file.

`-o update.xml` — Specifies the name of the results file. This is an XML file that contains the inventory/update results.

`-c nvmupdate.cfg` Specifies the name of the configuration file. This is a text file that contains descriptions of networking devices and firmware versions for those devices.

LEGAL

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

This document (and any related software) is Intel copyrighted material, and your use is governed by the express license under which it is provided to you. Unless the license provides otherwise, you may not use, modify, copy, publish, distribute, disclose or transmit this document (and related materials) without Intel's prior written permission. This document (and related materials) is provided as is, with no express or implied warranties, other than those that are expressly stated in the license.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

The products and services described may contain defects or errors which may cause deviations from published specifications.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.