NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2017-7936 Detail

Current Description

A stack-based buffer overflow issue was discovered in NXP i.MX 50, i.MX 53, i.MX 6ULL, i.MX 6UltraLite, i.MX 6SoloLite, i.MX 6Solo, i.MX 6DualLite, i.MX 6SoloX, i.MX 6Dual, i.MX 6Quad, i.MX 6DualPlus, i.MX 6QuadPlus, Vybrid VF3xx, Vybrid VF5xx, and Vybrid VF6xx. When the device is configured in security enabled configuration, SDP could be used to download a small section of code to an unprotected region of memory.

Source: MITRE
Description Last Modified: 08/07/2017
+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 6.3 MEDIUM
Vector: AV:P/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 0.4

Attack Vector (AV): Physical
Attack Complexity (AC): High
Privileges Required (PR): Low
User Interaction (UI): None

Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS v2.0 Severity and Metrics:

Base Score: 4.4 MEDIUM
Vector: (AV:L/AC:M/Au:N/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 3.4

Access Vector (AV): Local
Access Complexity (AC): Medium
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://www.securityfocus.com/bid/99966	**Third Party Advisory** **VDB Entry**
https://ics-cert.us-cert.gov/advisories/ICSA-17-152-02	**Third Party Advisory** **US Government Resource** **VDB Entry**

Technical Details

Vulnerability Type (View All)

- Buffer Errors (CWE-119)

Vulnerable software and versions Switch to CPE 2.2

Configuration 1

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf30nn151cku26_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf30nn151cku26:-:*:*:*:*:*:*:*

Configuration 2

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf30ns151cku26_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf30ns151cku26:-:*:*:*:*:*:*:*

Configuration 3

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf50nn151cmk40_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf50nn151cmk40:-:*:*:*:*:*:*:*

Configuration 4

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf50nn151cmk50_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf50nn151cmk50:-:*:*:*:*:*:*:*

Configuration 5

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf50ns151cmk40_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf50ns151cmk40:-:*:*:*:*:*:*:*

Configuration 6

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf50ns151cmk50_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf50ns151cmk50:-:*:*:*:*:*:*:*

Configuration 7

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf51nn151cmk50_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf51nn151cmk50:-:*:*:*:*:*:*:*

Configuration 8

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf51ns151cmk50_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf51ns151cmk50:-:*:*:*:*:*:*:*

Configuration 9

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf60nn151cmk40_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf60nn151cmk40:-:*:*:*:*:*:*:*

Configuration 10

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf60ns151cmk40_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf60ns151cmk40:-:*:*:*:*:*:*:*

Configuration 11

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf60nn151cmk50_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf60nn151cmk50:-:*:*:*:*:*:*:*

Configuration 12

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf60ns151cmk50_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf60ns151cmk50:-:*:*:*:*:*:*:*

Configuration 13

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf61nn151cmk50_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf61nn151cmk50:-:*:*:*:*:*:*:*

Configuration 14

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf61ns151cmk50_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf61ns151cmk50:-:*:*:*:*:*:*:*

Configuration 15

AND

OR

✱ cpe:2.3:o:nxp:vybrid_mvf62nn151cmk40_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:vybrid_mvf62nn151cmk40:-:*:*:*:*:*:*:*

Configuration 16

AND

OR

✱ cpe:2.3:o:nxp:i.mx_50_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_50:-:*:*:*:*:*:*:*

Configuration 17

AND

OR

✱ cpe:2.3:o:nxp:i.mx_53_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_53:-:*:*:*:*:*:*:*

Configuration 18

AND

OR

✱ cpe:2.3:o:nxp:i.mx_6ull_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_6ull:-:*:*:*:*:*:*:*

Configuration 19

AND

OR

✱ cpe:2.3:o:nxp:i.mx_6ultralite_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_6ultralite:-:*:*:*:*:*:*:*

Configuration 20

AND

OR

✱ cpe:2.3:o:nxp:i.mx_6sololite_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_6sololite:-:*:*:*:*:*:*:*

Configuration 21

AND

OR

✱ cpe:2.3:o:nxp:i.mx_6solo_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_6solo:-:*:*:*:*:*:*:*

Configuration 22

AND

OR

✱ cpe:2.3:o:nxp:i.mx_6duallite_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_6duallite:-:*:*:*:*:*:*:*

Configuration 23

AND

OR

✱ cpe:2.3:o:nxp:i.mx_6solox_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_6solox:-:*:*:*:*:*:*:*

Configuration 24

AND

OR

✱ cpe:2.3:o:nxp:i.mx_6dual_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_6dual:-:*:*:*:*:*:*:*

Configuration 25

AND

OR

✱ cpe:2.3:o:nxp:i.mx_6quad_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_6quad:-:*:*:*:*:*:*:*

Configuration 26

AND

OR

✱ cpe:2.3:o:nxp:i.mx_6quadplus_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_6quadplus:-:*:*:*:*:*:*:*

Configuration 27

AND

OR

✱ cpe:2.3:o:nxp:i.mx_6dualplus_firmware:-:*:*:*:*:*:*:*

OR

cpe:2.3:h:nxp:i.mx_6dualplus:-:*:*:*:*:*:*:*

✱ Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

Change History

2 change records found - show changes

QUICK INFO

CVE Dictionary Entry:

CVE-2017-7936

NVD Published Date:

08/07/2017

NVD Last Modified:

08/25/2017

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

Webmaster | Contact Us | Our Other Offices

GENERAL

NVD Dashboard
News
Email List
FAQ
Visualizations

VULNERABILITIES

Search & Statistics
Full Listing
Categories

Data Feeds
Vendor Comments

VULNERABILITY METRICS

CVSS V3 Calculator
CVSS V2 Calculator

PRODUCTS

CPE Dictionary
CPE Search
CPE Statistics
SWID

CONFIGURATIONS (CCE)

CONTACT NVD

OTHER SITES

Checklist (NCP) Repository
800-53 Controls
SCAP Validated Tools
SCAP
USGCB

SEARCH

Vulnerability Search
CPE Search

Information Technology Laboratory
National Vulnerability Database

Announcement and Discussion Lists
General Questions & Webmaster Contact
Email:nvd@nist.gov

Incident Response Assistance and Non-NVD Related Technical Cyber Security Questions:
US-CERT Security Operations Center
Email: soc@us-cert.gov
Phone: 1-888-282-0870

Sponsored by
DHS/NCCIC/US-CERT