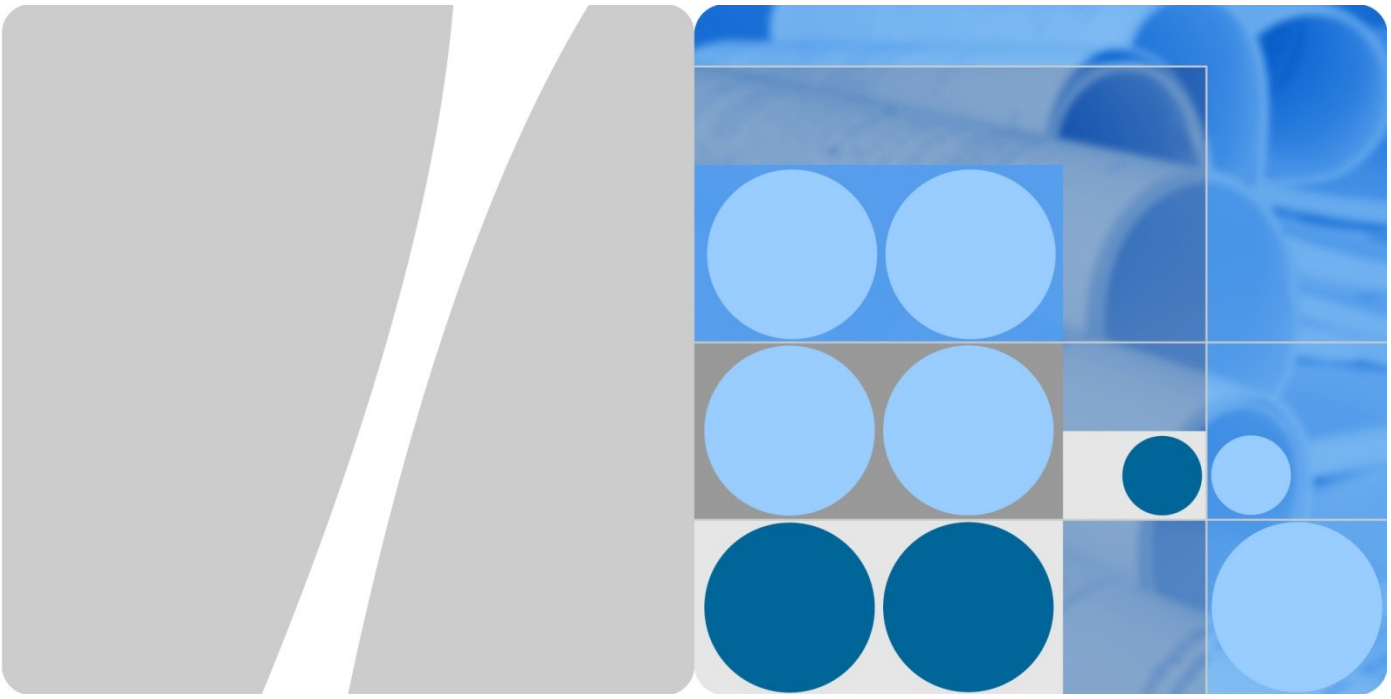


NE40E-M2

V800R011SPH032

Patch Release Notes

Issue **01**

Date 2020-08-10

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Change History

Issue	Date	Author	Description
01	2020-08-10	Gao Feng	This issue is the first official release.

Contents

Change History....ii

1 Patch Package Information....1

1.1 Product Name....1
1.2 Product Model....1
1.3 Patch Number....1
1.4 Release Date....1
1.5 Patch File Description....1
1.6 Product Version and Required Patches....2
1.7 Relationship Between Patches....2
1.7.1 V800R011C00SPC200....2
1.7.2 V800R011C10SPC100....3
1.8 Impact of Patch Installation....3
1.9 Precautions....3
1.10 Naming Rules for Patches....4

2 Resolved Issues....6

2.1 How to Obtain Issues Resolved....6

3 Installing the Patch....7

3.1 Installing the Patch....7
3.1.1 Preparing to Install....7
3.1.2 Installing the Patch....8
3.2 Verifying Patch Installation....8
3.2.1 NE40E-M2 V800R011C00SPC200....9
3.2.2 NE40E-M2 V800R011C10SPC100....9
3.3 Follow-up Procedures After Patch Installation....9

4 Rollback Procedure....10

4.1 How to Roll Back to the Previous State....10

5 Solutions to Common Problems During Patch Installation....11

5.1 A Message "Error: The system file should be in root directory." Is Displayed After the patch load all run Command Is Run to Load a Patch File....11
5.2 A Message "Error: The command is invalid in the current patch status." Is Displayed After the patch load all run Command Is Run to Load a Patch File....11

5.3 A Message "Error: The patch is incompatible with the existing patch." Is Displayed After the patch load all run Command Is Run to Load a Patch File....12
5.4 How Can I Set a Patch as That to Be Loaded at the Next Startup?....12
A Vulnerabilities Fixed....13

1 Patch Package Information

1.1 Product Name

HUAWEI NetEngine40E Series Universal Service Router

1.2 Product Model

NE40E-M2E, NE40E-M2F,NE40E-M2H, NE40E-M2K, NE40E-M2K-B

1.3 Patch Number

NE40E-M2 V800R011SPH032

1.4 Release Date

2020-08-10

1.5 Patch File Description

Table 1.1 Patch file description

File Name	File Description	File Size
NE40E-M2V800R011SPH032-C00SPC200.PAT	V800R011SPH032patch file	24,371,587 bytes
NE40E-M2V800R011SPH032-C10SPC100.PAT	V800R011SPH032patch file	17,105,283 bytes

1.6 Product Version and Required Patches

Product Version	Product Patch
NE40E-M2 V800R011C00SPC200	NE40E-M2V800R011SPH032-C00SPC200.PAT
NE40E-M2 V800R011C10SPC100	NE40E-M2V800R011SPH032-C10SPC100.PAT

1.7 Relationship Between Patches

Relationships between patches are classified as function inheritance or incremental relationships.

- Function inheritance relationship: If the latest patch resolves all issues that have been resolved in earlier patches, functions are inherited. Otherwise, functions are not inherited.
- Incremental relationship: If the latest patch can be directly installed on a device with earlier patches installed, the relationship between patches is considered an incremental relationship. Otherwise, the relationship between patches is considered a non-incremental relationship.

Before installing an incremental patch, doe not remove the existing historical patch on a device, which prevents triggering problems that have been resolved using the historical patch.

Before installation a non-incremental patch, note the following issues:

- If a device needs to be restarted or a software package needs to be upgraded, do not remove an existing historical patch from a device. Set the latest patch as the patch to be loaded at the next startup. After the device is restarted, the patch can take effect.
- If services keep running on a device, remove an existing historical patch from a device and then install the latest patch. During the historical patch removal and latest patch installation, problems that have been resolved using the historical patch may be triggered. Evaluate such risk before you operate the patches. Do not perform any operations on the device between uninstalling the earlier patches and installing the latest patch. Otherwise, services may be interrupted. For example, saving configurations causes the commands added in the patches to be lost.

1.7.1 V800R011C00SPC200

Table 1.2 Relationships between patches

Latest Patch	Earlier Patch	Function Inheritance Relationship	Incremental Relationship
V800R011SPH032	V800R011SPH029	Inheritance	Incremental

Latest Patch	Earlier Patch	Function Inheritance Relationship	Incremental Relationship
	V800R011SPH027	Inheritance	Incremental
	V800R011SPH025	Inheritance	Incremental
	V800R011SPH023	Inheritance	Incremental
	V800R011SPH020	Inheritance	Incremental
	V800R011SPH018	Inheritance	Incremental
	V800R011SPH016	Inheritance	Incremental
	V800R011SPH012	Inheritance	Incremental
	V800R011SPH006	Inheritance	Incremental
	V800R011SPH005	Inheritance	Incremental

1.7.2 V800R011C10SPC100

Table 1.3 Relationships between patches

Latest Patch	Earlier Patch	Function Inheritance Relationship	Incremental Relationship
V800R011SPH032	V800R011SPH029	Inheritance	Incremental
	V800R011SPH027	Inheritance	Incremental
	V800R011SPH026	Inheritance	Incremental
	V800R011SPH025	Inheritance	Incremental
	V800R011SPH023	Inheritance	Incremental
	V800R011SPH021	Inheritance	Incremental
	V800R011SPH020	Inheritance	Incremental
	V800R011SPH018	Inheritance	Incremental
	V800R011SPH016	Inheritance	Incremental

1.8 Impact of Patch Installation

See the **Solution Impact** and **Precautions for Installing the Patch** columns in the *NE40E-M2 V800R011SPH032 Issues Resolved*.

1.9 Precautions

2. It is acceptable if the patch file is loaded to boards asynchronously.
3. During patch installation or uninstallation, ensure that all boards in use have been registered. If any interface board is starting during patch installation or uninstallation, the patch installation or uninstallation will probably fail on this interface board.
4. Do not install the patch if the board CPU usage exceeds 70%. Otherwise, patch installation may fail.
5. Do not install the patch if the board memory usage exceeds 80%. Otherwise, the board may reset due to a failure to apply for memory. To check the memory and CPU usage, run the **display health** command in the system view.

```
[HUAWEI]display health
------------------------------------------------------------------------------
Slot   CPU         Usage     Memory    Usage(Used/Total)
17     MPU(Master) 5%        20%       1646MB/7929MB
2      LPU           7%        60%       1017MB/1684MB
19     SFU           3%        8%        80MB/980MB
------------------------------------------------------------------------------
```

6. The new function provided by the patch cannot be used if the patch is uninstalled. Therefore, to use the new function, do not uninstall the patch. If the patch needs to be upgraded, use the incremental patch loading mode.
7. When loading a patch that contains a YANG model change, ensure that no NETCONF session is in the configuration editing state. Otherwise, an unknown error may occur.

DANGER

In a scenario in which a user uses Telnet to access a NE40E-M2 through an interface on an interface board, if you want to restart the interface or power off and then power on the interface board or subcard where the interface resides for the installed patch to take effect, ensure that there is a backup Telnet connection to another interface board. If there is no backup Telnet connection, do not restart the interface or power off and then power on the interface board or subcard where the interface resides. Otherwise, the user will fail to access the NE40E-M2.

After the patch is installed and activated, you must restart the board or interface. For detailed procedures, see section 3.3.

1.10 Naming Rules for Patches

Patches are classified as hot patches and cold patches based on the impacts that patches have on user experience when they are activated and validated.

A hot patch (HP) does not affect user experience because it does not cause service interruptions when it is activated and validated.

A cold patch (CP) affects user experience because it causes service interruptions when it is activated and validated.

Naming rules for Accumulated Correction Updates (ACUs) are as follows:

8. For an ACU that is released based on the previous cold ACU, if the current ACU contains patches that would affect user experience when being activated and validated, the current ACU is a cold ACU and named SPCyyy.
9. For an ACU that is released based on the previous cold ACU, if the current ACU does not contain any patches that would affect user experience when being activated and validated, the current ACU is a hot ACU and named SPHyyy.

Naming rules for Emergency Correction Patches (ECPs) are as follows:

1. For an ECP that is released based on the previous ACU, if activating and validating the ECP would not affect user experience, the ECP is named as a hot ECP in the format of HPyyyy; if activating and validating the ECP would affect user experience, the ECP is named as a cold ECP in the format of CPyyyy.
2. The first y in HPyyyy or CPyyyy is fixed at 0, and the subsequent yyy is the same as yyy in SPCyyy or SPHyyy of the previous ACU. Therefore, an ECP is named in the format of HP0yyy or CP0yyy. If a calculated ECP name is the same as that of the previously released ECP, "yyy" in the newly calculated one increases by 1.

For example, after a cold ACU named SPC011 is released, the first hot ECP is named HP0011, and the next hot ECP is named HP0012. After a hot ACU named SPH012 is released, the first cold ECP is named CP0013 because the number 0012 has already been used by HP0012 for the same ACU.

Activating and validating a hot ACU or an ECP released based on the previous cold ACU and a later released hot ACU would not affect user experience. However, activating and validating a hot ACU or an ECP released based on an ACU earlier than the previous cold ACU or on a device that is not equipped with any patches would affect user experience. Therefore, comply with the precautions for activating and validating cold ACUs when performing these operations.

2 Resolved Issues

This section describes the issues that are resolved in V800R011 and precautions for installing the patch. For detailed information, see the *NE40E-M2 V800R011SPH032 Issues Resolved*.

CAUTION

Pay attention to the precautions for installing the patch. **The possible causes are as follows: Restart the device, perform an master/slave switchover, power off and then power on the board or subcard, reset the board or subcard, reconfigure the device, or add configurations. Exercise caution when performing this operation.**

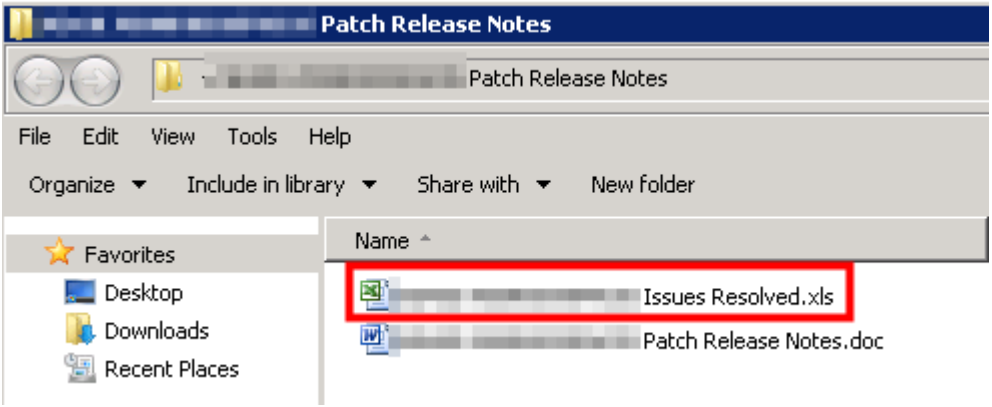
2.1 How to Obtain Issues Resolved

NOTE

The website does not support online browsing of Excel files. Therefore, you cannot view the *Issues Resolved* online. Download and view the list.

Step 1 Download the *Patch Release Notes* Zip package to the local host.

Step 2 Decompress the *Patch Release Notes* and view the *Issues Resolved*.



3 Installing the Patch

3.1 Installing the Patch

3.1.1 Preparing to Install

Before installing the patch, perform the following steps to make necessary preparations.

Step 2 Obtain the NE40E-M2 V800R011SPH032 patch from http://support.huawei.com.

Step 3 Verify the digital signature of the patch package.

To prevent the software package from being maliciously tampered with during transmission or storage, download the related digital signature file for integrity verification when downloading the software package.
After the software package is downloaded, verify the PGP digital signature of the software package by following the procedure in *OpenPGP Signature Verification Guide*. If the verification fails, do not use the software package. Contact Huawei technical support.
Before using the software package for installation or upgrade, verify the digital signature of the software package to ensure that the software package is not tampered with.
For carrier customers, visit https://support.huawei.com/carrier/digitalSignatureAction.
For enterprise customers, visit https://support.huawei.com/enterprise/en/tool/pgp-verify-TL1000000054.

Step 4 Run the **display version** command on the device to check whether the software version matches the patch version. For details, see section.1.6

```
<HUAWEI>display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 8.xxx (NE40E V800R0xxCxxSPCxxx)
```

Step 5 Upload the NE40E-M2V800R011SPH032-C10SPC100.PAT file to cfcard:/ using FTP in binary mode, after ensuring that the patch name does not conflict with any existing file name on the NE40E-M2.

Step 6 If the slave MPU or SRU exists, copy the patch to the slave MPU or SRU running the following command:

```
<HUAWEI> copy NE40E-M2V800R011SPH032-C10SPC100.PAT slave#cfcard:/
```

Step 7 Run the **display patch-information process verbose | include NO | exclude Running** command in the diagnostic view to check the patch unit status. If the following command

output is displayed, each patch unit is running properly. If a different command output is displayed, some patch units are not running properly. To troubleshoot this problem, contact Huawei R&D engineers.

```
[~HUAWEI-diagnose]display patch-information process verbose | include NO | exclude
Running
Info: It will take a long time if the content you search is too much or the string
you input is too long, you can press CTRL_C to break.
--------------------------------------------------------------------------------
-----
Slot-id  ProcId   State     PatchType Valid     PatchEffectiveTime
PatchFileName
--------------------------------------------------------------------------------
-----
--------------------------------------------------------------------------------
-----
```

CAUTION

The patch is large, and uploading the patch takes some time. If the CF card has sufficient space, you can upload the patch to the NE40E-M2 before uninstalling existing patches. If the patch name conflicts with an existing file name, modify the patch name before uploading the patch.

----End

3.1.2 Installing the Patch

CAUTION

Use the **patch load NE40E-M2V800R011SPH032-C10SPC100.PAT all run** command to install the patch. If you use other commands, some issues may fail to be resolved.

Run the **patch load NE40E-M2V800R011SPH032-C10SPC100.PAT all run** command to load, activate, and run the patch.

The system displays the patch installation results.

For example:

```
<HUAWEI> patch load NE40E-M2V800R011SPH032-C10SPC100.PAT all run
Info: Operating, please wait for a moment...done.
Info: Succeeded in running the patch.
```

3.2 Verifying Patch Installation

Run the **display version** command to verify that the system software version is correct.

```
<HUAWEI>display version
```

```
Huawei Versatile Routing Platform Software
VRP (R) software, Version 8.190 (NE40E V800R011C10SPC100)
Copyright (C) 2012-2019 Huawei Technologies Co., Ltd.
```

In the preceding command output, the characters in bold are the current system software version.

3.2.1 NE40E-M2 V800R011C00SPC200

```
<HUAWEI> display patch-information
Patch Package Name    :cfcard:/NE40E-M2V800R011SPH032-C00SPC200.PAT
Patch Package Version :V800R011SPH032
Patch Package State   :Running
Patch Package Run Time: 2020-08-10 10:57:30
```

3.2.2 NE40E-M2 V800R011C10SPC100

```
<HUAWEI> display patch-information
Patch Package Name    :cfcard:/NE40E-M2V800R011SPH032-C10SPC100.PAT
Patch Package Version :V800R011SPH032
Patch Package State   :Running
Patch Package Run Time: 2020-08-10 10:57:30
```

3.3 Follow-up Procedures After Patch Installation

After patch installation, check whether issues described in the *NE40E-M2 V800R011SPH032 Issues Resolved*.xlsx delivered with the patch release notes exist on the device. If any issues exist, perform operations listed in the corresponding "Operation Type for Patch Validation" and "Operation Type for Service Restoration " in the *NE40E-M2 V800R011SPH032 Issues Resolved*.xlsx. **The possible causes are as follows: Restart the device, perform an master/slave switchover, power off and then power on the board or subcard, reset the board or subcard, reconfigure the device, or add configurations. Exercise caution when performing this operation.**

4 Rollback Procedure

4.1 How to Roll Back to the Previous State

If patch installation fails and a rollback is necessary, perform the following steps to roll back to the previous state.

Step 8 Run the **display patch-information** command in the user view to check the patch running status.

Step 9 Run the **patch delete all** command in the user view to delete all patches.

Step 10 Run the **display patch-information** command in the user view to check whether the patches are still running. Ensure that the patches are not running.

----End

When the patch is being uninstalled, do not run any commands. Otherwise, services may become abnormal or the master main control board may be reset. After the patch is uninstalled, you are advised to log out all users who logged in through terminal tools.

5 Solutions to Common Problems During Patch Installation

5.1 A Message "Error: The system file should be in root directory." Is Displayed After the patch load all run Command Is Run to Load a Patch File.

Symptom

```
<HUAWEI>patch load $_install_mod/NE40E-M2V800R011SPHxxx.PAT all run
Info: Operating, please wait for a moment...
Error: The system file should be in root directory.
```

Solution

This problem occurs if a patch file to be loaded is not stored in the root directory of the master MPU. Therefore, to resolve this problem, copy the patch file to the root directory on the CF card before running the **patch load NE40E-M2V800R011SPH*xxx*.PAT all run** command in the user view.

5.2 A Message "Error: The command is invalid in the current patch status." Is Displayed After the patch load all run Command Is Run to Load a Patch File.

Symptom

```
<HUAWEI>patch load NE40E-M2V800R011SPHxxx.PAT all run
Info: Operating, please wait for a moment...
Error: The command is invalid in the current patch status.
```

Solution

This problem occurs if a patch has been installed and the patch is not in the running state. Therefore, to resolve this problem, run the **display patch-information** command in the user view to check whether a patch has been installed and whether the patch is in the running state.

```
<HUAWEI>display patch-information
Patch Package Name    :cfcard:/NE40E-M2V800R011SPHxxx.PAT
Patch Package Version :V800R011SPHxxx
Patch Package State   :Deactive
```

In this example, a patch has been loaded and the patch is not in the running state.

In this case, before loading the new patch, run the **patch load NE40E-M2V800R011SPH*xxx*.PAT all run** command in the user view to have the existing patch enter the running state or run the **patch delete all** command to delete the existing patch.

5.3 A Message "Error: The patch is incompatible with the existing patch." Is Displayed After the patch load all run Command Is Run to Load a Patch File.

Symptom

```
<HUAWEI>patch load NE40E-M2V800R011SPHxxx.PAT all run
Info: Operating, please wait for a moment...
Error: The patch is incompatible with the existing patch.
```

Solution

This problem occurs if the patch in the file to be loaded is not an incremental one of the existing patch on the device. Therefore, to resolve this problem, run the **patch delete all** command in the user view to delete the existing patch before loading the new patch.

5.4 How Can I Set a Patch as That to Be Loaded at the Next Startup?

A: Run the following commands on the master and slave main control boards:

```
<HUAWEI> startup patch cfcard:/NE40E-M2V800R011SPHxxx.PAT all
Info: Operating, please wait for a moment.....done.
Info: Succeeded in setting startup the patch.
```

A Vulnerabilities Fixed

You can query vulnerabilities at the National Vulnerability Database (NVD) website (http://web.nvd.nist.gov/view/vuln/search) by CVE ID.

A.1 V800R011C00SPC200

Software Name	Software Version	CVE Number	CVSS	Vulnerability Description	Solution Version
Zstandard	1.3.5	CVE-2019-11922	8.1	A race condition in the one-pass compression functions of Zstandard prior to version 1.3.8 could allow an attacker to write bytes out of bounds if an output buffer smaller than the recommended size was used.	V800R011SPH018

A.2 V800R011C10SPC100

Software Name	Software Version	CVE Number	CVSS	Vulnerability Description	Solution Version
python	2.7.17~3.8	CVE-2019-18348	6.1	An issue was discovered in urllib2 in Python 2.x through 2.7.17 and urllib in Python 3.x through 3.8.0. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the host component of a URL) followed by an HTTP header. This is similar to the CVE-2019-9740 query string issue and the CVE-2019-9947 path string issue. (This is not exploitable when glibc has CVE-2016-10739 fixed.)	V800R011SPH032

Software Name	Software Version	CVE Number	CVSS	Vulnerability Description	Solution Version
Libyang	1.0-r2	CVE-2019-20398	6.5	A NULL pointer dereference is present in libyang before v1.0-r3 in the function lys_extension_instances_free() due to a copy of unresolved extensions in lys_restr_dup(). Applications that use libyang to parse untrusted input yang files may crash.	V800R011SPH027
Libyang	1.0-r2	CVE-2019-20391	6.5	An invalid memory access flaw is present in libyang before v1.0-r3 in the function resolve_feature_value() when an if-feature statement is used inside a bit. Applications that use libyang to parse untrusted input yang files may crash.	V800R011SPH027
Libyang	1.0-r2	CVE-2019-20394	8.8	A double-free is present in libyang before v1.0-r3 in the function yyparse() when a type statement in used in a notification statement. Applications that use libyang to parse untrusted input yang files may be vulnerable to this flaw, which would cause a crash or potentially code execution.	V800R011SPH027
Libyang	1.0-r2	CVE-2019-19333	9.8	In all versions of libyang before 1.0-r5, a stack-based buffer overflow was discovered in the way libyang parses YANG files with a leaf of type "bits". An application that uses libyang to parse untrusted YANG files may be vulnerable to this flaw, which would allow an attacker to cause a denial of service or possibly gain code execution.	V800R011SPH027
Libyang	1.0-r2	CVE-2019-19334	9.8	In all versions of libyang before 1.0-r5, a stack-based buffer overflow was discovered in the way libyang parses YANG files with a leaf of type "identityref". An application that uses libyang to parse untrusted YANG files may be vulnerable to this flaw, which would allow an attacker to cause a denial of service or possibly gain code execution.	V800R011SPH027