47260 Red Hat Enterprise Linux 9 の nodejs:18 にポリシー機構を迂回されるなど複数の問題

CVSS 基本値	攻撃コード	登録日時	SID 危険度
7.5		2023/08/01	Medium
		更新日時	SID 影響範囲
		2023/08/01	リモート

CVE-2023-30581 CVE-2023-30588 CVE-2023-30589 CVE-2023-30590

更新情報

2023/08/01 コンテンツ 登録
2023/08/01 CVE-2023-30581, CVE-2023-30588, CVE-2023-30589, CVE-2023-30590 CVSS 登録

概要

Node.js は、スケーラブルなネットワークアプリケーションを構築するためのソフトウェアプラットフォームです。
Red Hat Enterprise Linux 9 の nodejs:18 モジュールは、実装上の原因で複数のセキュリティホールが存在します。
これらのセキュリティホールにより、ポリシー機構による制限を迂回され、policy.json へ定義した以外のモジュールを使用されるなどの攻撃を受ける可能性があります。

1. **7.5** **mainModule.proto の処理にポリシー機構を迂回される問題 (CVE-2023-30581)**
   Node.js は、mainModule.proto の処理が原因でセキュリティホールが存在します。
   このセキュリティホールにより、ポリシー機構による制限を迂回され、policy.json へ定義した以外のモジュールを使用される可能性があります。
2. **5.3** **crypto.X509Certificate API の処理にサービスを妨害される問題 (CVE-2023-30588)**
   Node.js は、crypto.X509Certificate API の処理が原因でセキュリティホールが存在します。
   このセキュリティホールを利用された場合、Node.js アプリケーションで組工された公開鍵を使用され X509 証明書を作成することによって、アプリケーションを不正に停止されサービスを妨害される可能性があります。
3. **7.5** **llhttp の処理に HTTP リクエストスマグリング攻撃を受ける問題 (CVE-2023-30589)**
   Node.js は、llhttp の処理が原因でセキュリティホールが存在します。
   このセキュリティホールを利用された場合、Node.js アプリケーションで組工された HTTP リクエストを処理することによって、HTTP リクエストスマグリング (Request Smuggling) 攻撃を受ける可能性があります。
   これは Node.js の llhttp の処理において、HTTP ヘッダフィールドの分割操作を適切に行っていないことが原因となります。
4. **5.3** **generateKeys API の処理に Diffie-Hellman 公開鍵を生成しない問題 (CVE-2023-30590)**
   Node.js は、generateKeys API の処理が原因でセキュリティホールが存在します。
   このセキュリティホールにより、秘密鍵を設定してある場合に crypto.createDiffieHellman の generateKeys API で Diffie-Hellman 公開鍵を生成しない可能性があります。

関連情報

Common Vulnerabilities and Exposures (CVE)
CVE-2023-30581
Common Vulnerabilities and Exposures (CVE)
CVE-2023-30588
Common Vulnerabilities and Exposures (CVE)
CVE-2023-30589
Common Vulnerabilities and Exposures (CVE)
CVE-2023-30590
Red Hat Linux Security Advisory
RHSA-2023:4330 Moderate: nodejs:18 security, bug fix, and enhancement update

影響を受ける製品

- **Red Hat Linux**
  Enterprise Linux 9
  Enterprise Linux EUS 9.2
  Enterprise Linux AUS 9.2
  Enterprise Linux 9.2 - 4 years of updates

確認方法

インストールされているバージョンを確認してください。 (下記の確認方法は一例です)

- **パッケージからインストールした場合の確認方法 (rpm)**
  ```
  # rpm -qa | grep [パッケージ名]
  ```

対処方法

Red Hat Linux
yum コマンドを使用して修正パッケージを適用してください。また rpm コマンドを使用する場合は、以下の修正パッケージを適用してください。

- **Red Hat Enterprise Linux 9**
  [SRPM]
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.src.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.src.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.src.rpm
  [x86_64]
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  [s390x]
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  [ppc64le]
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  [aarch64]
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
- **Red Hat Enterprise Linux EUS 9.2**
  [SRPM]
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.src.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.src.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.src.rpm
  [x86_64]
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  [s390x]
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  [ppc64le]
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.ppc64le.rpm
  [aarch64]
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
- **Red Hat Enterprise Linux AUS 9.2**
  [SRPM]
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.src.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.src.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.src.rpm
  [x86_64]
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.x86_64.rpm
- **Red HatEnterprise Linux 9.2 - 4 years of updates**
  [SRPM]
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.src.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.src.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.src.rpm
  [aarch64]
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.aarch64.rpm
  [s390x]
  nodejs-docs-18.16.1-1.module+el9.2.0.z+19424+78951f07.noarch.rpm
  nodejs-nodemon-2.0.20-2.module+el9.2.0.z+18497+a402347c.noarch.rpm
  nodejs-packaging-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-packaging-bundler-2021.06-4.module+el9.1.0+15718+e52ec601.noarch.rpm
  nodejs-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-debuginfo-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-debugsource-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-devel-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  nodejs-full-i18n-18.16.1-1.module+el9.2.0.z+19424+78951f07.s390x.rpm
  npm-9.5.1-1.18.16.1.1.module+el9.2.0.z+19424+78951f07.s390x.rpm

ベンダーの対処方法を適用しない場合の回避方法

適切な回避方法はありません。
回避方法については操作性/機能性などを制限することで回避される一時的なものであり、セキュリティホールが修正されたことにはなりません のでご注意ください。

更新履歴

2023/08/01 コンテンツ 登録

© 1998 - 2023 Cyber Security Cloud, Inc. All rights reserved.