NextStep_172.21.2.5

Mphasis Vulnerability Scan Report

Report generated by Nessus™ Tue, 27 Feb 2018 16:12:00 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

172.21.2.5

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	2	0	0	0

Scan Information

Start time:	Tue Feb 27 16:12:00 2018
End time:	Tue Feb 27 19:57:34 2018

Host Information

Netbios Name:	SRVAZRPOCMGRDB1
IP:	172.21.2.5
MAC Address:	00:0D:3A:31:85:34
OS:	Microsoft Windows Server 2016 Datacenter

Vulnerabilities

105730 - Security Update for .NET Core (January 2018)

Synopsis

The remote Windows host is affected by a .NET Core runtime vulnerability.

Description

The remote Windows host has an installation of .NET Core with a version less than 2.0.5. Therefore, the host is affected by multiple vulnerabilities :

- A security feature bypass in X509 Certificate Validation allows an attacker to present a certificate that is marked as invalid for a specific use, but a component uses it for that purpose. (CVE-2018-0786)

- A denial of service vulnerability exists due to improper processing of XML documents. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET application. A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to a .NET Core application. (CVE-2018-0764)

See Also

https://github.com/dotnet/announcements/issues/51

https://github.com/dotnet/announcements/issues/52

http://www.nessus.org/u?ebdb4bc7

http://www.nessus.org/u?6ee5ffe3

http://www.nessus.org/u?e1e826f0

http://www.nessus.org/u?9a103486

http://www.nessus.org/u?3759d74b

http://www.nessus.org/u?cf7d5ce3

Solution

Update to .NET Core Runtime version 1.09 / 1.1.6 / 2.0.5 or later.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2018-0786
CVE	CVE-2018-0764
XREF	OSVDB:172253
XREF	OSVDB:172259
XREF	IAVB:2018-B-0009

Plugin Information:

Published: 2018/01/10, Modified: 2018/02/08

Plugin Output

tcp/445

```
Path              : C:\program files\dotnet\shared\Microsoft.NetCore.App\2.0.3.25816\
Installed version : 2.0.3.25816
Fixed version     : 2.0.5.26021

Path              : C:\program files (x86)\dotnet\shared\Microsoft.NetCore.App\2.0.3.25816\
Installed version : 2.0.3.25816
Fixed version     : 2.0.5.26021
```

106190 - Oracle Java SE Multiple Vulnerabilities (January 2018 CPU)

Synopsis

The remote Windows host contains a programming platform that is affected by multiple vulnerabilities.

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 9 Update 4, 8 Update 161, 7 Update 171, or 6 Update 181. It is, therefore, affected by multiple vulnerabilities related to the following components :

- AWT
- Deployment
- Hotspot
- I18n
- Installer
- JCE
- JGSS
- JMX
- JNDI
- JavaFX
- LDAP
- Libraries
- Serialization

See Also

http://www.nessus.org/u?b3fb6d01

http://www.nessus.org/u?7986d2c2

http://www.nessus.org/u?68d74646

http://www.nessus.org/u?4f2226dc

http://www.nessus.org/u?726f7054

Solution

Upgrade to Oracle JDK / JRE 9 Update 4, 8 Update 161 / 7 Update 171 / 6 Update 181 or later. If necessary, remove any affected versions.

Note that an Extended Support contract with Oracle is needed to obtain JDK / JRE 6 Update 95 or later.

Risk Factor

High

CVSS v3.0 Base Score

8.3 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	102546
BID	102556
BID	102557
BID	102576
BID	102584
BID	102592
BID	102597
BID	102605
BID	102612
BID	102615
BID	102625
BID	102629
BID	102633
BID	102636
BID	102642
BID	102656
BID	102659
BID	102661
BID	102662
BID	102663
CVE	CVE-2018-2579
CVE	CVE-2018-2581
CVE	CVE-2018-2582
CVE	CVE-2018-2588
CVE	CVE-2018-2599
CVE	CVE-2018-2602
CVE	CVE-2018-2603

CVE	CVE-2018-2618
CVE	CVE-2018-2627
CVE	CVE-2018-2629
CVE	CVE-2018-2633
CVE	CVE-2018-2634
CVE	CVE-2018-2637
CVE	CVE-2018-2638
CVE	CVE-2018-2639
CVE	CVE-2018-2641
CVE	CVE-2018-2657
CVE	CVE-2018-2663
CVE	CVE-2018-2677
CVE	CVE-2018-2678
XREF	OSVDB:172895
XREF	OSVDB:172897
XREF	OSVDB:172898
XREF	OSVDB:172899
XREF	OSVDB:172900
XREF	OSVDB:172907
XREF	OSVDB:172908
XREF	OSVDB:172909
XREF	OSVDB:172910
XREF	OSVDB:172911
XREF	OSVDB:172912
XREF	OSVDB:172913
XREF	OSVDB:172914
XREF	OSVDB:172915
XREF	OSVDB:172916
XREF	OSVDB:172917
XREF	OSVDB:172918
XREF	OSVDB:172919
XREF	OSVDB:172920
XREF	OSVDB:172921
XREF	IAVA:2018-A-0031

Plugin Information:

Published: 2018/01/19, Modified: 2018/01/22

Plugin Output

tcp/445

```
The following vulnerable instance of Java is installed on the
```

```
remote host :

  Path              : C:\Program Files\Java\jdk1.8.0_91\jre
  Installed version : 1.8.0_91
  Fixed version     : 1.6.0_181 / 1.7.0_171 / 1.8.0_161 / 1.9.0_4
```