NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

July 2020, Edition 2.0

NETWORK INTELLIGENCE SECURITY ADVISORY

The major security news items of the month - major threats and breaches. The advisory also includes IOCs and remediation steps.

IN THIS EDITION:

Security Advisory Listing	Severity
A Read-Only Path Traversal vulnerability (CVE-2020-3452) within Web Services Interface of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defence (FTD) devices that was widely exploited in Hacking Campaigns.	Critical
A Remote Code Execution vulnerability (CVE-2020-1147) in Microsoft SharePoint Server, Microsoft .NET Framework, and Microsoft Visual Studio, was widely exploited in targeted Malware Attack and Hacking Campaigns.	Critical
Oracle Corporation released Critical Patch Updates (CPU) on July 2020, for Oracle Products such as Oracle WebLogic, Oracle Database, Oracle Solaris, Oracle MySQL, Oracle VirtualBox, and Oracle JAVA SE.	Critical
A Remote Code Execution vulnerability (CVE-2020-1350) within Windows DNS Server role implementation in Microsoft Windows Server products, was found more likely to be exploited in case of targeted Malware attacks.	Critical

ALSO INSIDE

Data Breach Highlights

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A Read-Only Path Traversal vulnerability (CVE-2020-3452) within Web Services Interface of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defence (FTD) devices that was widely exploited in Hacking Campaigns.

Severity: Critical

Date: July 24, 2020

IMPACT

The business impacts of this vulnerability are not limited to unauthorized access, data breach, financial loss, disruption in business operations affects organization reputation and breach of customer trust.

REMEDIATION

1. Immediately apply security patches for the vulnerability CVE-2020-3452, on Cisco ASA and Cisco FTD devices.

(Note:- Please find attached Excel sheet for quick access to Fix Release versions and our recommendations)

2. Ensure to check and fix misconfiguration issues in the web services file system of ASA or FTD devices.

3. We also recommend checking on the Command-Line Configuration Guide of Cisco ASA and Cisco FTD devices, for any further technical assistance with regards to configuration.

IMPORTANT

- Cisco ASA Software releases 9.5 and earlier, as well as Release 9.7, have reached the end of software maintenance. Customers are advised to migrate to a supported release.

INTRODUCTION

A Read-Only Path Traversal vulnerability (CVE-2020-3452) within Web Services Interface of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) devices, is widely exploited in Hacking Campaigns.

The vulnerability (CVE-2020-3452) is due to improper input validation of URLs in HTTP requests, which allows unauthenticated remote attacker to send a specifically crafted HTTP request containing directory traversal character sequences towards affected Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) devices.

On successful exploitation of this vulnerability (CVE-2020-3452) will allow a remote attacker to view arbitrary files within the web services file system on the affected Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) devices.

The web services file system is enabled when the ASA or FTD device is configured with either WebVPN or AnyConnect features. This vulnerability (CVE-2020-3452) cannot be used to obtain further access to ASA or FTD system files or underlying operating system (OS) files.

This vulnerability (CVE-2020-3452) poses a severe risk of a security breach followed by a data breach incident.

AFFECTED PRODUCTS

- Cisco ASA: 9.6 and earlier
- Cisco ASA: 9.7, 9.8, 9.9, 9.10, 9.12, 9.13, 9.14
- Cisco FTD: 6.2.2 and earlier
- Cisco FTD: 6.2.2, 6.2.3, 6.3.0, 6.4.0, 6.5.0, 6.6.0

READ

- Cisco Adaptive Security Appliance Software and Firepower ThreatDefense Software Web Services Read-Only Path Traversal Vulnerability
- CVE-2020-3452: Cisco Adaptive Security Appliance and Firepower Threat Defense Path Traversal Vulnerability
- POC | CVE-2020-3452, unauthenticated file read in Cisco ASA & Cisco Firepower

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A Remote Code Execution vulnerability (CVE-2020-1147) in Microsoft SharePoint server, Microsoft .NET Framework, and Microsoft Visual Studio, was widely exploited in targeted Malware Attack and Hacking Campaigns.

Severity: Critical

Date: July 21, 2020

IMPACT

The business impacts of this vulnerability are not limited to unauthorized access, data breach, financial loss, disruption in business operations affect organization reputation and breach of customer trust.

REMEDIATION

1. Immediately apply security patch for vulnerability CVE-2020-1147, to Microsoft SharePoint Server, .NET Framework, and Visual Studio products.

(Note:- Please find attached Excel sheet for quick access to the security patches)

2. We also recommend checking on the security guidelines for Microsoft SharePoint, Microsoft .NET, and Microsoft Visual Studio

INTRODUCTION

A Remote Code Execution vulnerability (CVE-2020-1147) in Microsoft SharePoint server, Microsoft .NET Framework, and Microsoft Visual Studio, is widely exploited in targeted Malware Attack and Hacking Campaign.

This vulnerability (CVE-2020-1147) is due to Microsoft SharePoint server, Microsoft .NET Framework, and Microsoft Visual Studio fails to check the source markup of XML file input, which allows remote attacker with low privilege to run arbitrary code in the context of the process responsible for deserialization of the XML content.

This vulnerability (CVE-2020-1147) poses a severe risk of security breach such as unauthorized access, and execution of disruptive malware like ransomware attack across enterprise-wide network.

The business impacts of this vulnerability are not limited to unauthorized access, data breach, financial loss, disruption in business operations, affects organization reputation, and breach of customer trust.

It is strongly recommended to immediately apply security patches for this vulnerability (CVE-2020-1147) on affected Microsoft Windows Servers and Workstations. We also recommend checking on the security guidelines for Microsoft SharePoint, Microsoft .NET, and Microsoft Visual Studio.

AFFECTED PRODUCTS

- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Enterprise Server 2013 Service Pack 1
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server 2010 Service Pack 2
- Microsoft Visual Studio 2019 version 16.6 (includes 16.0 - 16.5)
- Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
- Microsoft .NET Core 2.1/3.1
- Microsoft .NET Framework 3.5/3.5.1/ 4.5.2/4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2/4.8
- Microsoft .NET Framework 2.0/3.0 Service Pack 2

READ

- CVE-2020-1147 | .NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Oracle Corporation released Critical Patch Updates (CPU) on July 2020, for Oracle Products such as Oracle WebLogic, Oracle Database, Oracle Solaris, Oracle MySQL, Oracle VirtualBox, and Oracle JAVA SE.

Severity: Critical

Date: July 16, 2020

IMPACT

On successful exploitation of these vulnerabilities would allow a remote attacker to gain unauthorized access, exfiltrate data, and cause disruption in business operations.

REMEDIATION

1. Immediately apply available security patches for Oracle WebLogic, Oracle Database, Oracle Solaris, Oracle MySQL, Oracle VirtualBox, and Oracle JAVA SE.

2. Please refer attached Excel sheet for more details on exploitable CVE IDs, and quick access to the security patches for respective Oracle products.

INTRODUCTION

Oracle Corporation released Critical Patch Updates (CPU) on April 2020, for Oracle products such as WebLogic, Oracle Database, Oracle Solaris, Oracle MySQL, Oracle VM VirtualBox, Oracle JAVA SE, and many other Oracle products.

Easily exploitable vulnerabilities in Oracle WebLogic Server (CVE-2020-14625, CVE-2020-14644, CVE-2020-14645, CVE-2020-14687), Oracle Database Server (CVE-2020-2969, CVE-2020-2978), Oracle Solaris (CVE-2019-5489, CVE-2020-14542), Oracle MySQL Server (CVE-2020-14663, CVE-2020-14678, CVE-2020-14697, CVE-2020-14643, CVE-2020-14651, CVE-2020-14641), Oracle VM VirtualBox (CVE-2020-14628, CVE-2020-14711, CVE-2020-14629, CVE-2020-14703, CVE-2020-14704, CVE-2020-14712), and Oracle Java (CVE-2020-14621), would allow remote unauthenticated attacker with network access might compromise Oracle products.

On successful exploitation of these vulnerabilities would allow remote attacker to take complete control over Oracle products, gain unauthorized access to sensitive data, and execute ransomware like disruptive attack on enterprise wide network.

AFFECTED PRODUCTS

- Oracle WebLogic 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0,14.1.1.0.0.
- Oracle Database 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c.
- Oracle Solaris 11.
- Oracle MySQL 4.0.12 and prior, 5.6.48 and prior, 5.7.30 and prior, 7.3.29 and prior, 7.4.28 and prior, 7.5.18 and prior, 7.6.14 and prior, 8.0.20 and prior.
- Oracle VirtualBox Prior to 5.2.44, prior to 6.0.24, prior to 6.1.12.
- Oracle Java SE: 7u261, 8u251, 11.0.7, 14.0.1.
- Oracle Java SE Embedded: 8u251

READ

- Oracle Critical Patch Update Advisory - July 2020
- Critical Patch Update for July 2020 Now Available

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A Remote Code Execution vulnerability (CVE-2020-1350) within Windows DNS Server role implementation in Microsoft Windows Server products, was found more likely to be exploited in case of targeted Malware attacks.

Severity: Critical

Date: July 15, 2020

IMPACT

The business impacts of this vulnerability are not limited to unauthorized access, data breach, financial loss, disruption in business operations, affects organization reputation, and breach of customer trust.

REMEDIATION

1. Immediately apply the security patch for the vulnerability CVE-2020-1350, on Microsoft Windows Server products.

(Note:- Please find attached Excel sheet for quick access to the security patches)

2. Incase applying security patches is not possible due to production issues, then kindly implement this workaround to fix vulnerability CVE- 2020-1350, on Microsoft Windows Server products.

INTRODUCTION

A Remote Code Execution vulnerability (CVE-2020-1350) within Windows DNS Server (a core networking component) in Microsoft Windows Server products, found more likely to be exploited in targeted Malware Attacks.

This vulnerability (CVE-2020-1350) is due to the Microsoft Windows DNS Server role implementation that fails to properly handle DNS related requests, which allows unauthenticated, remote attacker to send maliciously crafted DNS queries towards vulnerable Windows DNS Server role implemented on affected Microsoft Windows Servers.

This vulnerability (CVE-2020-1350) poses a severe risk of a security breach, such as rapid distribution of disruptive malware like ransomware attack across the enterprise-wide network. This vulnerability being wormable in nature, can allow unauthenticated remote attacker to claim entire IT infrastructure as hostage for demanding big ransom amount through targeted ransomware attack, and makes it harder to recover from the demand caused.

The business impacts of this vulnerability are not limited to unauthorized access, data breach, financial loss, disruption in business operations, affects organization reputation, and breach of customer trust.

It is strongly recommended to immediately apply security patches for this vulnerability (CVE-2020-1350) on affected Microsoft Windows Servers. Incase applying security patches is not possible due to production issues, then kindly implement this workaround immediately to mitigate the risk.

AFFECTED PRODUCTS

- All versions of Microsoft Windows Server products, including Core Installations, are affected.

READ

- CVE-2020-1350 | Windows DNS Server Remote Code Execution Vulnerability
- July 2020 Security Update: CVE-2020-1350 Vulnerability in Windows Domain Name System (DNS) Server
- SIGRed – Resolving Your Way into Domain Admin: Exploiting a 17 Year-old Bug in Windows DNS Servers

NETWORK INTELLIGENCE
Global cybersecurity provider

NEWSLETTER

July 2020, Edition 2.0

DATA BREACH HIGHLIGHTS

Cognizant had suffered a security breach followed by Maze ransomware attack, and later confirmed data breach

June 18, 2020

- IT giant Cognizant confirms data breach after ransomware attack

JOOMLA, open-source content management system (CMS) known for publishing web content, developed by Open Source Matters suffered data leakage

June 01, 2020

- Content management system Joomla hit by data breach

Indian video on demand giant ZEE5 suffered security breach

June 07, 2020

- ZEE5 allegedly hacked by 'Korean hackers', customer info at risk