October 27, 2020

Monthly Vulnerabilities Bulletin - October 2020

Cyberint

TABLE OF CONTENTS

OVERVIEW

These vulnerabilities were observed to be Critical in October 2020.

Cyberint's Research Team recommends to patch and take the necessary steps immediately.

- CVE-2020-16952 - Sharepoint Remote Code Execution
- CVE-2020-16898 - "Bad Neighbor" \ "Ping of Death"
- CVE-2020-15999 - Chrome Freetype 0day
- CVE-2020-8243 - Pulse Secure Arbitrary Code Execution

CVE-2020-16952 - MICROSOFT SHAREPOINT AUTHENTICATED REMOTE CODE EXECUTION VULNERABILITIES

INTRODUCTION

On Tuesday, October 13, as part of the October 2020 Patch Tuesday release, Microsoft has published a security advisory for CVE-2020-16952, a server-side include (SSI) vulnerability in Microsoft SharePoint.

The bug is exploitable by an authenticated user with page creation privileges, which is a standard permission in SharePoint, and allows the leaking of an arbitrary file, notably the application's web.config file, which can be used to trigger remote code execution (RCE) via .NET deserialization

Several RCE vulnerabilities were found and reported to Microsoft, impacting Sharepoint.

All these vulnerabilities were binded under a single CVE.

IMPACT

Full Remote Command Execution over the Sharepoint server and highly potential lateral movement within the organization.

Impacted versions, include, but not limited to:

- Microsoft SharePoint Enterprise Server 2016

- Microsoft SharePoint Server 2019
- Microsoft SharePoint Foundation 2013 Service Pack 1

Exploits available? Yes - Metasploit and Python.

Exploitation observed in the wild? No.

CVSS Score: 8.6

DETECTION

Defenders can detect this exploit variant by identifying HTTP headers containing the string:

```
<!-- 360Vulcan might not always appear -->
360Vulcan: <**form runat="server"** /><!--#include virtual="/web.config"-->
```

As well as auditing SharePoint page creations.

RECOMMENDATIONS

The October 2020 SharePoint Security update addresses the vulnerability by correcting how SharePoint checks the source markup of application packages:

Please see:

- KB4486694 for SharePoint 2013
- KB4486677 for SharePoint 2016
- KB4486676 for SharePoint 2019

The patch for CVE-2020-16952 enables `blockServerSideIncludes` in the `VerifyControlOnSafeList()` call within `CreateChildControls()`:

```
- EditingPageParser.VerifyControlOnSafeList(this._dataSourcesString.Trim(),
null, base.Web, false);
+ EditingPageParser.VerifyControlOnSafeList(this._dataSourcesString.Trim(),
null, base.Web, true);
internal static void VerifyControlOnSafeList(string dscXml,
RegisterDirectiveManager registerDirectiveManager, SPWeb web, bool
blockServerSideIncludes = false)
```

- [1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16952
- [2] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16952
- [3] https://srcincite.io/advisories/src-2020-0022/

CVE-2020-16898 - "BAD NEIGHBOR"

INTRODUCTION

CVE-2020-16898, also dubbed 'Bad Neighbor', is a critical remote code execution (RCE) vulnerability that arises when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets using the Recursive DNS Server Option ("Option Type 25") and an even length field value.

Due to the nature of this vulnerability, exploits are not easy to craft, and currently result in a Blue Screen of Death (BSOD), but they become available in the coming days the threat could elevate especially considering that this could be "Wormable", that being a threat that could propagate from victim to victim.

CVSS Score: 9.0

IMPACT

An unauthenticated attacker who successfully exploits this vulnerability could gain the ability to execute code on the target server or client with high privileges. To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote windows computer.

Impacted versions include, but are not limited to:

- Windows 10
- Windows Server 2019
- Windows Server Core

With affected builds including 1903, 1909 and 2004.

DETECTION

This vulnerability can be detected with a simple heuristic that parses all incoming ICMPv6 traffic, looking for packets with an ICMPv6 Type field of '134' – indicating Router Advertisement – and an ICMPv6 Option field of '25' – indicating Recursive DNS Server (RDNSS). If this RDNSS option has a length field value that is even, the heuristic could drop or flag the associated packet as a potential "Bad Neighbor" exploit attempt.

RECOMMENDATIONS

- Apply the latest October 2020 Cumulative Update from Microsoft that includes a security update [1] specifically for this vulnerability.
- If it is not possible to patch, the following command can be used on vulnerable machines to disable ICMPv6 RDNSS (for Windows build 1709 and above), replacing `*INTERFACENUMBER*` with the appropriate network interface number:

```
netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=disable
```

(Note, this change can be reverted by replacing `disable` with `enable`)

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898

CVE-2020-15999 - CHROME FREETYPE 0DAY

INTRODUCTION

On October 20, 2020, Ben Hawkes of Google's Project Zero warned Chrome users that Google had observed active exploitation of a zero-day in Chrome's implementation of FreeType, a popular open-source font rendering library. As of October 20, the Chrome team has a new release out that includes a fix for the zero-day vulnerability, which is listed as a heap buffer overflow.

The CVE-2020-15999 flaw is a memory corruption bug that resides in the FreeType font rendering library, which is included in standard Chrome releases.

The researchers did not disclose technical details about the attacks exploiting the CVE-2020-15999 in the wild to avoid mass exploitation from threat actors.

IMPACT

Exploits available? Potentially yes, although not found, Google has mentioned that is aware of reports that an exploit for CVE-2020-15999 exists in the wild.

CVSS Score: 4

DETECTION

Detection steps were not released by Google or observed.

RECOMMENDATIONS

Upgrade Google Chrome to the latest stable version (86.0.4240.111) as quickly as possible.

[1] https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_20.html

[2] https://twitter.com/benhawkes/status/1318640422571266048

CVE-2020-8238

INTRODUCTION

A vulnerability in Pulse Secure admin web interface could allow an authenticated attacker to upload custom template to perform an arbitrary code execution.

Although considered Critical, exploitation is considered as Low due to the need to authenticate.

IMPACT

CVSS Score: 7.2

Impacted Pulse Secure versions, include, but not limited to:

- Pulse Connect Secure (PCS) 9.1Rx or below
- Pulse Policy Secure (PPS) 9.1Rx or below

DETECTION

Defenders should look for new page creations in the Admin Web Console.

RECOMMENDATIONS

- Restrict admin web console to either Internal or Management interface and disable access from Internet. For step by step instruction, refer to KB44589
- Implement 2FA or MFA based configuration administrators.
- Add realm level restrictions for admin realms and roles to provide additional protection. For more info, refer to Access Restrictions under General Access Management guide.
- Upgrade to the following versions:
  - Pulse Connect Secure 9.1R8.2
  - Pulse Policy Secure 9.1R8.2