VIRSEC SECURITY RESEARCH LAB

EXPERT VULNERABILITY ANALYSIS

VULNERABILITY REPORT

CVE-2020-25476: LIFERAY CMS PORTAL (BLIND PERSISTENT XSS)
CVE-2020-10658: PROOFPOINT INSIDER THREAT MANAGEMENT SERVER (RCE)
CVE-2020-8287: NODE.JS (HTTP REQUEST SMUGGLING)
CVE-2021-21234: SPRING BOOT ACTUATOR LOG VIEW (DIRECTORY TRAVERSAL)
CVE-2020-4917: IBM CLOUD PAK (CSRF/ RCE)
CVE-2020-5146: CONFUSED DEPUTY: SONIC WALL SMA100 (OS COMMAND INJECTION)

VOLUME 1, 2021

VIRSEC

Vulnerability Research Report

Volume 1, 2021 Report
Security Research Team

VIRSEC

Table of Contents

Scope

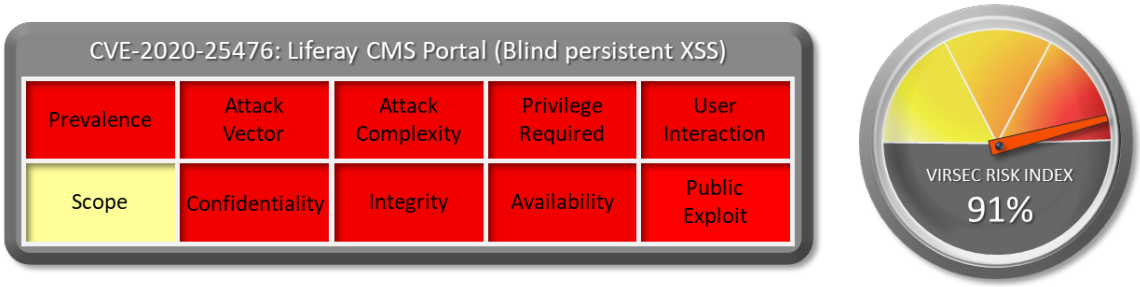
A total of 315 new vulnerabilities were reported for the week of 01/04/2021 to 01/10/2021. This document talks about 6 high impact vulnerabilities that were reported in this period, their affected version, vulnerability details and how VSP can protect users from the debilitating effects of these vulnerabilities.

- CVE-2020-25476: Liferay CMS Portal (Blind persistent XSS)
- CVE-2020-10658: Proofpoint Insider Threat Management Server (RCE)
- CVE-2020-8287: Node.js (HTTP Request Smuggling)
- CVE-2021-21234: Spring Boot Actuator Log view (Directory Traversal)
- CVE-2020-4917: IBM Cloud Pak (CSRF/ RCE)
- CVE-2020-5146: Confused Deputy: Sonic Wall SMA100 (OS Command Injection)

1 CVE-2020-25476: Liferay CMS Portal (blind persistent XSS)

1.1 Vulnerability Summary

Liferay CMS Portal version 7.1.3 and 7.2.1 have a blind persistent cross-site scripting (XSS) vulnerability in the username parameter to Calendar. An attacker can insert the malicious payload on the username, last name or surname fields of its own profile, and the malicious payload will be injected and reflected in the calendar of the user who submitted the payload. An attacker could escalate its privileges in case an admin visits the calendar that injected the payload.



1.2 Affected Version

Liferay CMS Portal version 7.1.3 and 7.2.1

1.3 CVSS Score

The CVSS Base score of this vulnerability has not been assigned yet.

1.4 Vulnerability Attribution

This vulnerability was disclosed by Casey Erdmann, Giuseppino Cadeddu, and Simone Cinti.

1.5 Risk Impact

A content management system (CMS) is software that enables non-technical users to store, organize and publish web content easily. Liferay is an open-source enterprise portal which is free and mainly used to enable corporate extranet and intranet. It is a robust web application platform written in Java and offers a host of features useful for the development of portals and websites. According to Builtwith, Liferay is deployed on ~54K websites.

An exploit is not publicly available but given the disclosure, it is very easy to construct one.

1.6 Virsec Security Platform (VSP) Support:

VSP-Web would be able to protect against such reflected Cross Site Scripting vulnerabilities.

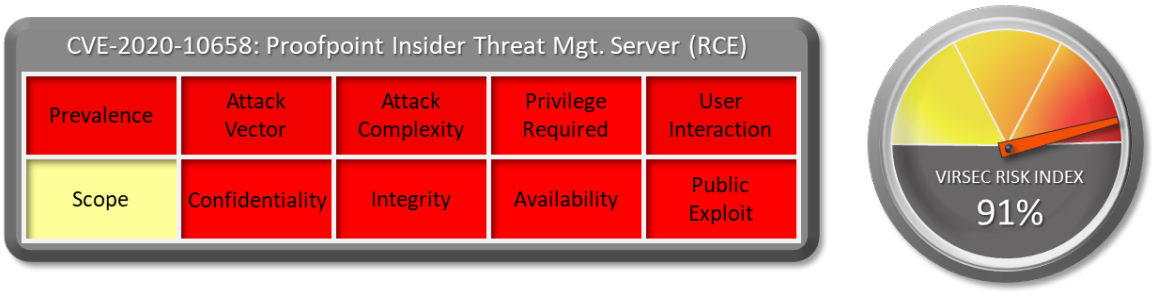
1.7 Reference Links:

- https://github.com/community-security-team/liferay-portal/compare/7.1.3-ga4...7.1.3-cumulative.patch
- https://nvd.nist.gov/vuln/detail/CVE-2020-25476
- https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/119318646

2 CVE-2020-10658: Proofpoint Insider Threat Management Server (RCE)

2.1 Vulnerability Summary

The Proofpoint Insider Threat Management Server (formerly ObserveIT Server) before 7.9.1 contains a vulnerability in the ITM application server's WriteImage API. The vulnerability allows an anonymous remote attacker to execute arbitrary code with local administrator privileges. The vulnerability is caused by improper deserialization.



2.2 Affected Version

The Proofpoint Insider Threat Management Server (formerly ObserveIT Server) before 7.9.1

2.3 CVSS Score

The CVSS Base score of this vulnerability is 9.8 Critical. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

2.4 Vulnerability Attribution

This vulnerability is disclosed by undisclosed sources.

2.5 Risk Impact

Proofpoint Insider Threat Management Server detect risky insider activity and prevent data loss from the endpoint. It also simplifies response to insider threat and data loss incidents. It defends enterprise against authorized users acting maliciously, negligently or unknowingly. And we correlate user activity and data movement to protect you from insider-led data breaches. Plus, we detect risky behavior in real-time to give you easy to understand evidence of wrongdoing.

An RCE in Proofpoint Insider Threat Management Server can lead to severe consequences. Insider Threat detection can be completely compromised.

An exploit is not publicly available but given the disclosure, it is very easy to construct one.

2.6 Virsec Security Platform (VSP) Support:

VSP-Host monitors processes that are spawned which are not part of a set of whitelisted process. Any attempt to execute new command or unknown binary would be denied by VSP-Host's Process Monitoring capability.

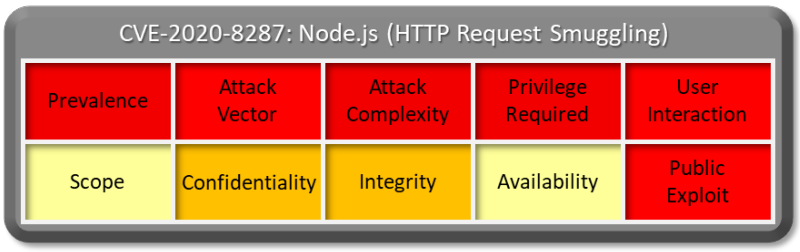
2.7 Reference Links:

- https://nvd.nist.gov/vuln/detail/CVE-2020-10658
- https://www.proofpoint.com/us/security/security-advisories/pfpt-sa-2020-0003

3 CVE-2020-8287: Node.js (HTTP Request Smuggling)

3.1 Vulnerability Summary

Node.js server allow two copies of a header field in an HTTP request (for example, two Transfer-Encoding header fields). In this case, Node.js identifies the first header field and ignores the second. This can lead to HTTP Request Smuggling.



3.2 Affected Version

Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1.

3.3 CVSS Score

CVSS Base score of this vulnerability is 6.5 Medium. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

3.4 Vulnerability Attribution

This vulnerability is disclosed by user “Piao” of HackerOne.

3.5 Risk Impact

Node.js is an application runtime environment that enables using JavaScript for building server-side applications that have access to the operating system, file system, and everything else to be fully functional. Among other server-side technologies, Node stands out with its speed, and intensive data exchange. It is a JavaScript runtime built on Chrome's V8 JavaScript engine. It uses an event-driven, non-blocking I/O model that makes it lightweight and efficient. Node. js can handle many concurrent requests. This is the main reason it quickly became popular among developers and large companies. Some users of Node.js are Netflix, Walmart, UBER, PAYPAL, LinkedIn etc.

HTTP Parameter smuggling allows an attacker to bypass security controls, gain unauthorized access to sensitive data, and directly compromise other application users

A publicly disclosed exploit is available here.

3.6 Virsec Security Platform (VSP) Support:

VSP-Host monitors processes that are spawned which are not part of a set of whitelisted process. Any attempt to execute new command or unknown binary would be denied by VSP-Host’s Process Monitoring capability.

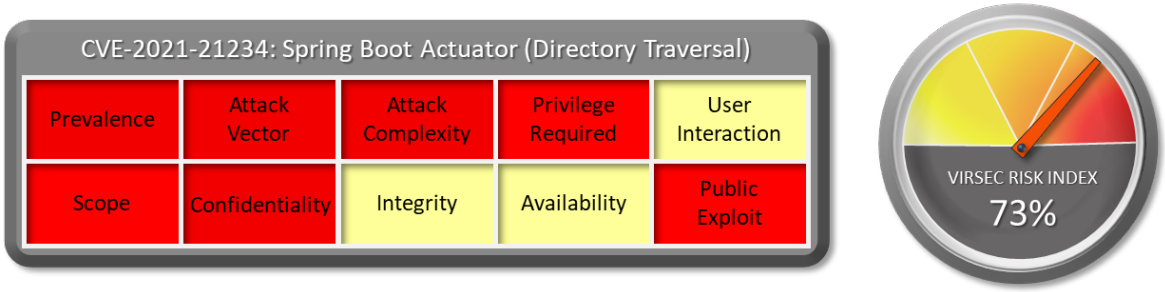
3.7 Reference Links:

- https://nvd.nist.gov/vuln/detail/CVE-2020-8287
- https://hackerone.com/reports/1002188

4 CVE-2021-21234: Spring Boot Actuator Log View (Directory Traversal)

4.1 Vulnerability Summary

The nature of this library is to expose a log file directory via admin (spring boot actuator) HTTP endpoints. Both the filename to view and a base folder (relative to the logging folder root) can be specified via request parameters. While the filename parameter was checked to prevent directory traversal exploits (so that `filename=../somefile` would not work), the base folder parameter was not sufficiently checked, so that `filename=somefile&base=../` could access a file outside the logging base directory).



4.2 Affected Version

Spring Boot Actuator Log View before version 0.2.13

4.3 CVSS Score

NVD Base score of this vulnerability is 7.7 High. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

4.4 Vulnerability Attribution

This vulnerability is fixed by user “lukashinsch” in Git Hub.

4.5 Risk Impact

In short, Spring Boot Actuator is one of the sub-projects of Spring Boot, which adds monitoring and management support for your applications running in production. It exposes various HTTP or JMX endpoints you can interact with. Spring Boot is an open-source Java-based framework used to create a Micro Service. It is developed by Pivotal Team and is used to build stand-alone and production ready spring applications.

If a web server or web application is vulnerable to directory traversal attack, the attacker can exploit the vulnerability to reach the root directory and access restricted files and directories. An attacker may use directory traversal to download server configuration files, which contain sensitive information and potentially expose more server vulnerabilities. Ultimately, the attacker may access confidential information or even get full control of the server.

An exploit is not publicly available but given the disclosure, it is very easy to construct one.

4.6 Virsec Security Platform (VSP) Support:

VSP-Web can block directory traversal attacks deterministically.

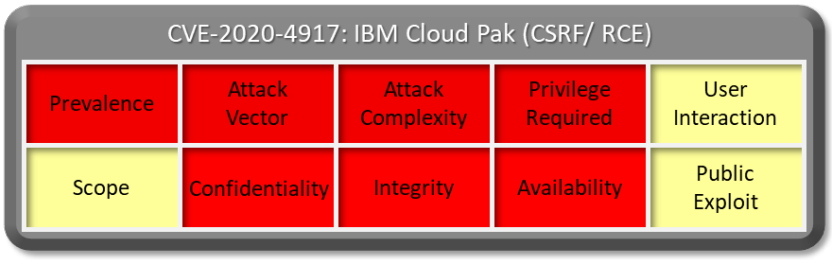
4.7 Reference Links:

- https://nvd.nist.gov/vuln/detail/CVE-2021-21234
- https://github.com/lukashinsch/spring-boot-actuator-logview/commit/1c76e1ec3588c9f39e1a94bf27b5ff56eb8b17d6

5 CVE-2020-4917: IBM Cloud Pak (CSRF)

5.1 Vulnerability Summary

IBM Cloud Pak System is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.



5.2 Affected Version

IBM Cloud Pak System 2.3

5.3 CVSS Score

The CVSS Base score of this vulnerability is 8.8 High. CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

5.4 Vulnerability Attribution

This vulnerability has not been attributed which may mean it is being exploited in the wild.

5.5 Risk Impact

IBM Cloud® Paks are AI-powered software for hybrid cloud that can help you fully implement intelligent workflows in your business to accelerate digital transformation. IBM Cloud Paks tap into the power of IBM Watson® to apply AI to your business to predict and shape future outcomes, automate complex processes, optimize your employees' time, and create more meaningful and secure customer experiences. Built on Red Hat® OpenShift®, you can develop applications once and deploy them anywhere on any cloud. In addition, you can integrate security across the breadth of your IT estate and automate your operations with management visibility. IBM Cloud Paks have a common foundation of enterprise components that accelerate development, deliver seamless integration, and help enhance collaboration and efficiency.

In a successful CSRF attack, the attacker causes the victim user to carry out an action unintentionally. For example, this might be to change the email address on their account, to change their password, or to make a funds transfer. Depending on the nature of the action, the attacker might be able to gain full control over the user's account. If the compromised user has a privileged role within the application, then the attacker might be able to take full control of all the application's data and functionality.

A publicly disclosed vulnerability is not available currently.

5.6 Virsec Security Platform (VSP) Support:

VSP-Web can protect against CSRF attacks. VSP-Host monitors processes that are spawned which are not part of a set of whitelisted process. Any attempt to execute new command or unknown binary would be denied by VSP-Host's Process Monitoring capability.

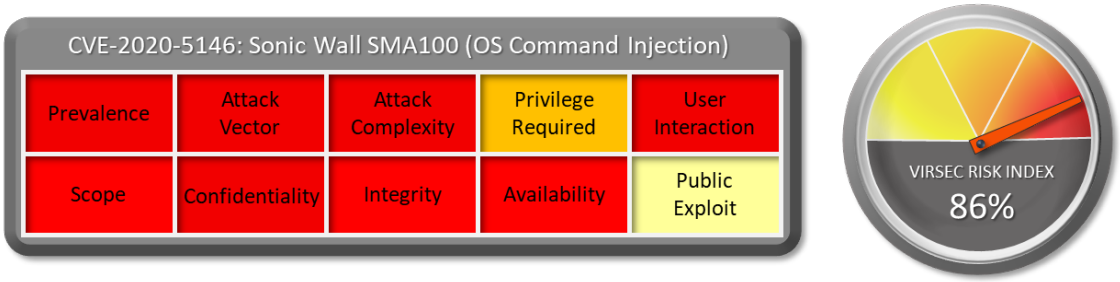
5.7 Reference Links:

- https://nvd.nist.gov/vuln/detail/CVE-2020-4917
- https://www.ibm.com/support/pages/node/6393554

6 CONFUSED DEPUTY: CVE-2020-5146: SonicWall SMA100 (OS Command Injection)

6.1 Vulnerability Summary

A vulnerability in SonicWall SMA100 appliance allow an authenticated management-user to perform OS command injection using HTTP POST parameters.



6.2 Affected Version

This vulnerability affected SMA100 Appliance version 10.2.0.2-20sv and earlier.

6.3 CVSS Score

CVSS Base score of this vulnerability is not available currently. This vulnerability is still being evaluated by NVD.

6.4 Vulnerability Attribution

This vulnerability is reported by Erik De Jong.

6.5 Risk Impact

SonicWall SMA is a unified secure access gateway that enables organizations to provide anytime, anywhere and any device access to mission critical corporate resources. SMA100 gives businesses with up to 250 users an affordable, secure remote access solution that is easy to deploy, use and manage. With multiple layers of security through policy-enforced access control to applications after establishing user and device identity and trust, a SonicWall SMA 100 Series means users can work from anywhere with security everywhere.

The consequences of a command injection attack can be very serious. An attacker can execute arbitrary commands with elevated privileges. With this ability they can take over the remote server.

A publicly disclosed vulnerability is not available currently.

6.6 Virsec Security Platform (VSP) Support:

VSP-Web can protect against OS Command Injection attacks. VSP-Host monitors processes that are spawned which are not part of a set of whitelisted process. Any attempt to execute new command or unknown binary would be denied by VSP-Host's Process Monitoring capability.

6.7 Reference Links:

- https://nvd.nist.gov/vuln/detail/CVE-2020-5146
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0022
- ttps://support.kaspersky.com/KART/3.1/en-US/130230.htm