CVE 2021-43557

Overview:

The uri-block plugin in Apache APISIX before 2.10.2 uses $request_uri without verification. The $request_uri is the full original request URI without normalization. This makes it possible to construct a URI to bypass the block list on some occasions. For instance, when the block list contains "^/internal/", a URI like `//internal/` can be used to bypass it. Some other plugins also have the same issue. And it may affect the developer's custom plugin.

CVS-Scope	7.5 (NVD)
Severity	HIGH
Communication	Apache APISIX
Vulnerability type	Path traversal in request_uri variable
Influence version	Before 2.10.2

Vulnerability patch: https://github.com/apache/apisix/pull/5458/commits/caeb1c97976068acb6223d899571de3e2ca7967a.

PoC: https://github.com/xvnpw/k8s-CVE-2021-43557-poc.

CVE 2021-44077

Overview:

Zoho ManageEngine ServiceDesk Plus before 11306, ServiceDesk Plus MSP before 10530, and SupportCenter Plus before 11014 are vulnerable to unauthenticated remote code execution. This is related to /RestAPI URLs in a servlet, and ImportTechnicians in the Struts configuration.

CVS-Scope	9.8 (NVD)
Severity	CRITICAL
Communication	SupportCenter Plus, ServiceDesk Plus MSP, ServiceDesk Plus
Vulnerability type	RCE
Influence version	• ServiceDesk Plus with versions **10527 till 10529** • SupportCenter Plus with versions **11012 and 11013** • ServiceDesk Plus MSP with versions **10527 till 10529**

PoC: https://github.com/horizon3ai/CVE-2021-44077.

Vulnerability patch:

CVE-2021-40539

Overview:

Zoho ManageEngine ADSelfService Plus version 6113 and prior is vulnerable to REST API authentication bypass with resultant remote code execution.

CVS-Scope	9.8 (NVD)
Severity	CRITICAL
Communication	ADSelfService Plus
Vulnerability type	RCE
Influence version	< 6113

POC:

- https://www.synacktiv.com/en/publications/how-to-exploit-cve-2021-40539-on-manageengine-adselfservice-plus.html
- https://github.com/DarkSprings/CVE-2021-40539

CVE 2021-38647

Overview:

By removing the authentication header, an attacker can issue an HTTP request to the OMI management endpoint that will cause it to execute an operating system command as the root user. This vulnerability was patched in OMI version 1.6.8-1 (released September 8th 2021)

CVS-Scope	9.8 (NVD)
Severity	CRITICAL
Communication	Microsoft OMI Management Interface
Vulnerability type	RCE

Influence version	< 1.6.8-1

PoC: https://github.com/AlteredSecurity/CVE-2021-38647.

Vulnerability patch: https://github.com/microsoft/omi/compare/v1.6.8-1...master.

CVE-2021-44228

Overview:

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Apache Log4j2 versions 2.0-alpha1 through 2.16.0, excluding 2.12.3, did not protect from uncontrolled recursion from self-referential lookups. When the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, $${ctx:loginId}), attackers with control over Thread Context Map (MDC) input data can craft malicious input data that contains a recursive lookup, resulting in a StackOverflowError that will terminate the process. This is also known as a DOS (Denial of Service) attack.

CVS-Scope	10 (NVD)
Severity	CRITICAL
Communication	Apache Log4j2
Vulnerability type	Deserialization of Untrusted Data
Influence version	2.15.0

PoC: https://github.com/logpresso/CVE-2021-44228-Scanner

CVE-2021-26295:

Overview:

Apache OFBiz has unsafe deserialization before 17.12.06. An unauthenticated attacker can use this vulnerability to successfully take over Apache OFBiz.

The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to insecure input validation when processing serialized data. A remote attacker can pass specially crafted data to the application and execute arbitrary code on the target system.

Successful exploitation of this vulnerability may result in complete compromise of vulnerable system

CVS-Scope	9.8 (NVD)
Severity	CRITICAL
Communication	Apache Ofbiz
Vulnerability type	Deserialization of Untrusted Data
Influence version	version <= 17.12.06

PoC: https://github.com/r0ckysec/CVE-2021-26295

CVE-2020-5902:

Overview:

In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.

CVS-Scope	9.8 (NVD)
Severity	CRITICAL
Communication	Apache Ofbiz

Vulnerability type	Path Traversal
Influence version	BIG-IP **version 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1**

PoC: https://github.com/yassineaboukir/CVE-2020-5902

CVE-2021-42237:

Overview:

Sitecore XP 7.5 Initial Release to Sitecore XP 8.2 Update-7 is vulnerable to an insecure deserialization attack where it is possible to achieve remote command execution on the machine. No authentication or special configuration is required to exploit this vulnerability.

CVS-Scope	9.8 (NVD)
Severity	CRITICAL
Communication	Sitecore XP
Vulnerability type	Deserialization of Untrusted Data
Influence version	Report.ashx page of Sitecore XP 7.5 to 7.5.2, 8.0 to 8.0.7, 8.1 to 8.1.3, and 8.2 to 8.2.7

PoC: https://github.com/PinkDev1/CVE-2021-42237