|  |  |  |
| --- | --- | --- |
|  | **بسمه‌تعالی** |  |
|  |  |  |
| ده‌ها آسیب‌پذیری در افرونه‌های Jenkins |
| خبر آسیب‌پذیری |
|  |
|  | **شناسه سند** Maher\_14010413**نوع سند** گزارش فنی**شماره نگارش** 0.1**تاریخ نگارش** 13/04/1401**طبقه‌بندی سند** **عادی** |
|  |
|  | تهران، خیابان شهید بهشتی، نرسیده به قائم مقام فراهانی، پلاک 267، سازمان فناوری اطلاعات ایران |
|  | 42650000 (021) |  | 42650000 (021) |  | cert.ir |

|  |  |
| --- | --- |
|  | فهرست مطالب |

[1 مقدمه 3](#_Toc106625502)

[2 جزئیات آسیب‌پذیری 3](#_Toc106625503)

[3 محصولات تحت تأثیر 6](#_Toc106625504)

[4 توصیه‌های امنیتی 7](#_Toc106625505)

[5 منابع خبر 7](#_Toc106625506)

# مقدمه

تیم امنیتی جنکینز[[1]](#footnote-1) ده‌ها نقص امنیتی را افشا کردند که چندین افزونه[[2]](#footnote-2) مربوط به سرور اتوماسیون جنکینز را تحت تاثیر قرار می‌دهد، این در حالی است که برای بیشتر این آسیب‌پذیری‌ها تاکنون وصله‌ای ارائه نشده است.

# جزئیات آسیب‌پذیری

جنکینز محبوب‌ترین سرور اتوماسیون منبع باز[[3]](#footnote-3) است که توسط [[4]](#footnote-4)CloudBees و انجمن جنکینز پشتیبانی می‌شود. این ابزار با [زبان جاوا](https://fa.wikipedia.org/wiki/%D8%AC%D8%A7%D9%88%D8%A7) و در جهت ادغام دائم و یکپارچه‌سازی برنامه نویسی، طراحی و ساخته شده است، همچنین پلاگین‌های مختلفی را برای ساخت، تست، تحلیل، نصب و غیره برای هر پروژه ارائه می‌دهد. جنکینز صدها هزار نصب فعال در سراسر جهان با بیش از یک میلیون کاربر دارد. شدت آسیب‌پذیری‌ها از کم تا بالا متغیر است.

| **شناسه آسیب‌پذیری** | **جزئیات آسیب‌پذیری** |
| --- | --- |
| **CVE-2022-34777** | آسیب‌پذیری XSS ذخیره شده در افزونه GitLab با شدت بالا |
| **CVE-2022-34778** | آسیب‌پذیری XSS در افزونه TestNG Results با شدت بالا |
| **CVE-2022-34779** | آسیب‌پذیری در افزونه XebiaLabs XL Release مربوط دسترسی به مجوزهای خواندن و نوشتن توسط مهاجم جهت شمارش شناسه‌های (IDs) در Jenkins با شدت متوسط |
| **CVE-2022-34780 (CSRF) و CVE-2022-34781** | آسیب‌پذیری CSRF در افزونه XebiaLabs XL Release با شدت متوسط |
| **CVE-2022-34782** | آسیب‌پذیری requests-plugin مربوط به بررسی نادرست مجوزها در افزونه XebiaLabs XL Release با شدت متوسط |
| **CVE-2022-34783** | آسیب‌پذیری XSS ذخیره شده در افزونه Plot Plugin با شدت بالا |
| **CVE-2022-34784** | آسیب‌پذیری XSS ذخیره شده در افزونه build-metrics با شدت بالا |
| **CVE-2022-34785** | آسیب‌پذیری مربوط به عدم بررسی مجوزهای دسترسی در افزونه build-metrics با شدت متوسط |
| **CVE-2022-34786** | آسیب‌پذیری XSS ذخیره شده در افزونه Rich Text Publisher با شدت بالا |
| **CVE-2022-34787** | آسیب‌پذیری XSS در افزونه Project Inheritance با شدت بالا |
| **CVE-2022-34788** | آسیب‌پذیری XSS ذخیره شده در افزونه Matrix Reloaded با شدت بالا |
| **CVE-2022-34789** | آسیب‌پذیری CSRF در افزونه Matrix Reloaded با شدت متوسط |
| **CVE-2022-34790** | آسیب‌پذیری XSS ذخیره شده در افزونه eXtreme Feedback Panel با شدت بالا |
| **CVE-2022-34791** | آسیب‌پذیری XSS ذخیره شده در افزونه Validating Email Parameter با شدت بالا |
| **CVE-2022-34792 (CSRF), CVE-2022-34793 (XXE), CVE-2022-34794** | آسیب‌پذیری مربوط به عدم بررسی مجوزهای دسترسی در افزونه Recipe  با شدت بالا |
| **CVE-2022-34795** | آسیب‌پذیری XSS ذخیره شده در افزونه Deployment Dashboard با شدت بالا |
| **CVE-2022-34796** | آسیب‌پذیری مربوط به عدم بررسی مجوزهای دسترسی در افزونه Deployment Dashboard با شدت متوسط |
| **CVE-2022-34797 (CSRF), CVE-2022-34798 (missing authorization)** | آسیب‌پذیری CSRF  و نقص مربوط به عدم بررسی مجوزهای دسترسی در افزونه Deployment Dashboard با شدت متوسط |
| **CVE-2022-34799** | آسیب‌پذیری مربوط به نحوه ذخیره‌سازی پسورد در قالب متن در افزونه Deployment Dashboard با شدت کم |
| **CVE-2022-34800 (storage), CVE-2022-34801 (transmission)** | آسیب‌پذیری مربوط به نحوه ذخیره‌سازی توکن‎‌ها در قالب متن در افزونه Build notifications با شدت پایین |
| **CVE-2022-34802** | آسیب‌پذیری مربوط به نحوه ذخیره‌ محتوای محرمانه در قالب متن در افزونه RocketChat Notifier با شدت پایین |
| **CVE-2022-34803 (storage), CVE-2022-34804 (transmission)** | آسیب‌پذیری مربوط به نحوه ذخیره‌ API Key در قالب متن در افزونه OpsGenie با شدت متوسط |
| **CVE-2022-34805** | آسیب‌پذیری مربوط به نحوه ذخیره‌ رمز‌های عبور در قالب متن در افزونه Skype notifier با شدت پایین |
| **CVE-2022-34806** | آسیب‌پذیری مربوط به نحوه ذخیره‌ رمز‌های عبور در قالب متن در افزونه Jigomerge  با شدت پایین |
| **CVE-2022-34807** | آسیب‌پذیری مربوط به نحوه ذخیره‌ رمز‌های عبور در قالب متن در افزونه Elasticsearch Query با شدت پایین |
| **CVE-2022-34808** | آسیب‌پذیری مربوط به نحوه ذخیره‌سازی توکن‎‌ها در قالب متن در افزونه Cisco Spark با شدت پایین |
| **CVE-2022-34809** | آسیب‌پذیری مربوط به نحوه ذخیره‌ رمز‌های عبور در قالب متن در افزونهRQM  با شدت پایین |
| **CVE-2022-34810** | آسیب‌پذیری مربوط به عدم بررسی مجوزهای دسترسی در افزونه RQM  با شدت متوسط |
| **CVE-2022-34811** | آسیب‌پذیری مربوط به عدم بررسی مجوزهای دسترسی در افزونه XPath Configuration Viewer با شدت متوسط |
| **CVE-2022-34812 (CSRF), CVE-2022-34813 (missing permission check)** | آسیب‌پذیری CSRF  و نقص مربوط به عدم بررسی مجوزهای دسترسی در افزونه XPath Configuration Viewer با شدت متوسط |
| **CVE-2022-34814** | آسیب‌پذیری requests-plugin مربوط به بررسی نادرست مجوزها در افزونه Request Rename Or Delete با شدت متوسط |
| **CVE-2022-34815** | آسیب‌پذیری CSRF در افزونه Request Rename Or Delete با شدت متوسط |
| **CVE-2022-34816** | آسیب‌پذیری مربوط به نحوه ذخیره‌ رمز‌های عبور در قالب متن در افزونهHPE Network Virtualization  با شدت پایین |
| **CVE-2022-34817 (CSRF), CVE-2022-34818 (missing authorization)** | آسیب‌پذیری CSRF  و نقص مربوط به عدم بررسی مجوزهای دسترسی در افزونه Failed Job Deactivator با شدت متوسط |

# محصولات تحت تأثیر

افزونه‌های آسیب‌پذیر و نسخه‌های آنها در ادامه آورده شده‌اند:

* **Build Notifications Plugin**up to and including 1.5.0
* **build-metrics Plugin**up to and including 1.3
* **Cisco Spark Plugin**up to and including 1.1.1
* **Deployment Dashboard Plugin**up to and including 1.0.10
* **Elasticsearch Query Plugin**up to and including 1.2
* **eXtreme Feedback Panel Plugin**up to and including 2.0.1
* **Failed Job Deactivator Plugin**up to and including 1.2.1
* **GitLab Plugin**up to and including 1.5.34
* **HPE Network Virtualization Plugin**up to and including 1.0
* **Jigomerge Plugin**up to and including 0.9
* **Matrix Reloaded Plugin**up to and including 1.1.3
* **OpsGenie Plugin**up to and including 1.9
* **Plot Plugin**up to and including 2.1.10
* **Project Inheritance Plugin**up to and including 21.04.03
* **Recipe Plugin**up to and including 1.2
* **Request Rename Or Delete Plugin**up to and including 1.1.0
* **requests-plugin Plugin**up to and including 2.2.16
* **Rich Text Publisher Plugin**up to and including 1.4
* **RocketChat Notifier Plugin**up to and including 1.5.2
* **RQM Plugin**up to and including 2.8
* **Skype notifier Plugin**up to and including 1.1.0
* **TestNG Results Plugin**up to and including 554.va4a552116332
* **Validating Email Parameter Plugin**up to and including 1.10
* **XebiaLabs XL Release Plugin**up to and including 22.0.0
* **XPath Configuration Viewer Plugin**up to and including 1.1.1

# توصیه‌های امنیتی

از تعداد 25 افزونه آسیب‌پذیر که به آنها اشاره شد تنها 4 افزونه وصله شده‌اند ‌و برای سایر افزونه‌ها در حال حاضر وصله‌ای منتشر نشده است. افزونه‌های وصله شده و نسخه آنها در جدول زیر آورده شده است:

|  |  |
| --- | --- |
| **محصول آسیب‌پذیر** | **نسخه وصله شده** |
| GitLab Plugin | 1.5.35 |
| requests-plugin Plugin | 2.2.17 |
| TestNG Results Plugin | 555.va0d5f66521e3 |
| XebiaLabs XL Release Plugin | 22.0.1 |

# منابع خبر

[1] https://www.jenkins.io/security/advisory/2022-06-30/

[2] https://securityaffairs.co/wordpress/132836/security/jenkins-plugins-zero-day-flaws.html

1. Jenkins [↑](#footnote-ref-1)
2. plugins [↑](#footnote-ref-2)
3. open-source [↑](#footnote-ref-3)
4. یک شرکت تولیدکننده نرم‌افزارهای سازمانی است که در اوایل سال 2010 تاسیس شده است [↑](#footnote-ref-4)