URGENT ACTION RECOMMENDED

RELEASED TUESDAY, 17 NOVEMBER 2026

November CSPU: Volume Holds at 655 Patches, but Java4Shell Puts the Java Runtime Itself at Risk

Summary and analysis of the November Critical Security Patch Update (CSPU)

For Waratek customers and prospects

Key findings, Oracle CSPU November 2026

The November 2026 Critical Security Patch Update includes 655 new security patches, covering 640 unique CVEs, across 21 product families. As in prior CSPUs, a single vulnerability can appear in more than one risk matrix when it affects several products. Highlights include:

655	**46%**	**6**	**1**
New security patches across 21 product families	303 patches remotely exploitable without authentication	Vulnerabilities at the maximum CVSS score of 10.0	Confirmed exploited flaw in this release (CISA KEV)

- **655 new security patches**, down about 3 percent from 673 in September and well below the 1,295 in October's quarterly Critical Patch Update. November is the third largest CSPU Oracle has issued, behind August (943) and September (673), and the second consecutive monthly decline since the August record.
- **303 of the 655 patches**, 46 percent of the release, address vulnerabilities Oracle classifies as remotely exploitable without authentication. That share is up from 37 percent in September (247 of 673) and is back to just under half, as in August.
- **Six vulnerabilities again carry the maximum CVSS base score of 10.0**, and all six require no authentication and are reachable over HTTP. Five sit in Oracle Fusion Middleware: Oracle Access Manager's Admin Console (CVE-2026-114835) and Authentication Engine (CVE-2026-91500 and CVE-2026-91510), Oracle Platform Security for Java (CVE-2026-114824), and Oracle WebLogic Server's TopLink Integration component (CVE-2026-91569). The sixth, CVE-2026-114784, sits in

the Platform Security component of Oracle Business Intelligence Enterprise Edition. In all, 62 entries, about 9.5 percent of the release, score 9.0 or higher.

- **Java SE receives 11 patches**, up from 3 in September, and Oracle rates all 11 as remotely exploitable without authentication. The highest Oracle score is 8.1, but that entry, CVE-2026-114938, is the HotSpot memory corruption flaw disclosed by Calif.io as Java4Shell. Calif rates it 9.2 under CVSS 4.0 and has demonstrated unauthenticated remote code execution against widely deployed Java applications, and CISA issued an alert on 17 November urging organizations to patch immediately. See the Java4Shell section below.
- **Hyperion is by far the largest family at 267 patches**, 107 of them unauthenticated, more than two and a half times September's 102 and about 41 percent of the whole release. It has no 10.0, but its ceiling is 9.9 and 11 of its 12 entries at 9.0 or above require no authentication, including five at 9.8 in the Infrastructure Technology and Planning products.
- **Fusion Middleware receives 71 patches**, down from 153 in September, but 53 of them are unauthenticated, 16 entries score 9.0 or higher, and 15 of those require no authentication. WebLogic Server adds a new TopLink Integration component with a 10.0 and three 9.8s, alongside further unauthenticated 9.8s in its Core component over SOAP and over T3 and IIOP.
- **Supply Chain jumps from 19 patches to 74**, concentrated in Oracle AutoVue, which carries a 9.9 that requires authentication and four unauthenticated 9.8s. Database Server has only 7 patches, but its ceiling rises from 8.8 in September to 9.9 on three authenticated entries.
- **E-Business Suite falls to 71 patches from 159**, with 19 unauthenticated and the same 9.8 ceiling. PeopleSoft receives 13 patches, 6 unauthenticated, and its ceiling returns to 9.8 after September's 8.8.
- **One vulnerability patched in this release is confirmed exploited.** CVE-2026-111497, a flaw in the Google Brotli decoder as embedded in Node.js, was added to the CISA Known Exploited Vulnerabilities catalog on 27 October and appears in Oracle's matrices for PeopleSoft PeopleTools, Communications Diameter Signaling Router and Communications Unified Assurance, each at 9.8 and unauthenticated. No other vulnerability in the release, including Java4Shell, has been publicly confirmed as exploited in the wild as of publication.
- **The practical threat picture is also shaped by October.** Exploitation attempts against an unauthenticated E-Business Suite SQL injection patched in the October CPU, CVE-2026-101767, were recorded within a week, and Oracle issued three out-of-cycle Security Alerts, on 21 October for CVE-2026-91403, on 24 October for CVE-2026-114820, and on 25 October for the PHP2Shell flaws CVE-2026-109618 and CVE-2026-109619, which CISA has since added to the KEV catalog. Previously disclosed WebLogic, PeopleSoft and E-Business Suite flaws from earlier in the year also remain exploited.

Patch volume by product family

Product family	Patches	Remote, no auth	Highest CVSS
Oracle Hyperion	267	107	9.9
Oracle Supply Chain	74	36	9.9
Oracle E-Business Suite	71	19	9.8
Oracle Fusion Middleware	71	53	**10.0**

Product family	Patches	Remote, no auth	Highest CVSS
Oracle Communications	31	21	9.8
Oracle Analytics	29	9	**10.0**
Oracle Siebel CRM	19	9	8.8
Oracle PeopleSoft	13	6	9.8
Oracle Financial Services Applications	11	1	7.5
Oracle Java SE	11	11	8.1
Oracle Virtualization (VirtualBox)	11	3	8.6
Oracle MySQL	10	3	9.8
Oracle REST Data Services	8	5	9.8
Oracle Database Server	7	3	9.9
Oracle Commerce	6	6	7.5
Oracle Enterprise Manager	5	3	9.1
Oracle Application Testing Suite	3	1	8.8
Oracle Autonomous Health Framework	3	3	9.1
Oracle APEX	2	2	9.8
Oracle Construction and Engineering	2	2	7.5
Oracle JD Edwards	1	0	6.5
Total	**655**	**303**	**10.0**

Source: Oracle Critical Security Patch Update Advisory, November 2026, published 17 November 2026. Counts are new security patches, not unique CVEs; the 655 patches correspond to 640 unique CVEs.

Family level analysis

Oracle Hyperion

Hyperion carries 267 patches this month, 107 of them unauthenticated, which makes it the largest family in the release by a wide margin. In September it was the third largest at 102 patches, concentrated in Financial Management's Security component. This month the volume is spread across Infrastructure Technology (76 patches), Financial Close Management (69), Planning (53) and Data Relationship Management (43), with smaller contributions from Profitability and Cost Management (13) and Financial Management (9).

No Hyperion entry reaches 10.0, but 12 score 9.0 or higher. The highest, CVE-2026-114978 at 9.9 in Financial Management's Security component, requires authentication. The other 11 are all unauthenticated: five at 9.8, namely CVE-2026-115048 in Infrastructure Technology's Common Security component, CVE-2026-115047 and CVE-2026-115080 in its Installation and Configuration component, CVE-2026-115089 in Planning's Application Development Framework and CVE-2026-115086 in Planning's Security component over RMI; one at 9.6 (CVE-2026-114785); two at 9.3 (CVE-2026-115139 and CVE-2026-114956); and three at 9.1 (CVE-2026-127362 and CVE-2026-127369 in Financial Close Management's Reconciliation Manager, the second over Oracle Net, and CVE-2026-115050). Hyperion

estates that are reachable from outside the application tier should be prioritized alongside Fusion Middleware.

Oracle Fusion Middleware

Fusion Middleware carries 71 patches this month, 53 of them unauthenticated, a much lighter release than September's 153 but still home to five of the six maximum-severity findings. All five score a full 10.0, require no authentication and are reachable over HTTP: CVE-2026-114835 in Oracle Access Manager's Admin Console, CVE-2026-91500 and CVE-2026-91510 in its Authentication Engine, CVE-2026-114824 in Oracle Platform Security for Java's Centralized Thirdparty Jars component, and CVE-2026-91569 in Oracle WebLogic Server's TopLink Integration component.

Identity infrastructure is disproportionately represented again, as it was with September's Internet Directory and Identity Manager findings. Access Manager contributes 14 patches, including the three 10.0s above, a further unauthenticated 9.3 in the Authentication Engine (CVE-2026-91507), and eight more unauthenticated entries between 7.2 and 8.7 over HTTP, SAML, LDAP and TCP.

WebLogic Server contributes 8 patches, 7 of them at 9.4 or above. The new TopLink Integration component carries the 10.0 plus three unauthenticated 9.8s, CVE-2026-91570 and CVE-2026-91583 over HTTP and CVE-2026-91585 over TCP. The Core component adds two further unauthenticated 9.8s, CVE-2026-91456 over SOAP and CVE-2026-91470 over T3 and IIOP, the same deserialization-prone channels behind past WebLogic remote code execution campaigns, and a 9.4 over HTTP, CVE-2026-91469. Elsewhere in the family, Service Delivery Platform's Messaging Enabler (CVE-2026-114826) is an unauthenticated 9.8 over SOAP, Application Development Framework's Security Framework (CVE-2026-91618) and Managed File Transfer's MFT Runtime Server (CVE-2026-8763) are unauthenticated 9.1s, and Oracle Service Bus's Core component (CVE-2026-91561, 9.6) requires authentication.

Separately from this month's new disclosures, WebLogic Server's HTTP proxy plug-in remains the most consequential confirmed risk in this family. CVE-2026-21962, patched in January and added to the CISA Known Exploited Vulnerabilities catalog on 24 August after a mass exploitation campaign, should still be independently verified on any deployment fronted by the Apache or IIS plug-in. This month's Oracle HTTP Server entry for the plug-in (CVE-2026-9545, a curl component rated 7.5) is a separate and lower-severity item.

Oracle E-Business Suite

E-Business Suite falls to 71 patches from September's 159, with 19 unauthenticated and the same 9.8 ceiling, across versions 12.2.3 through 12.2.15. Six entries score 9.0 or higher, all six are unauthenticated and all six are reachable over HTTP. Four reach 9.8: CVE-2026-114880 in Document Management and Collaboration's Attachments component, CVE-2026-114924 in Oracle Application Object Library's Core component, CVE-2026-114925 in Oracle Applications Framework's REST Services component, and CVE-2026-114863 in Oracle Universal Work Queue's Media Integration component. The other two are a 9.3 in Oracle Mobile Field Service's Admin UI (CVE-2026-101691) and a 9.1 in Document Management and Collaboration (CVE-2026-114881).

The Application Object Library finding deserves attention beyond its score. Oracle's October CPU listed CVE-2026-101767, an unauthenticated SQL injection that can chain to remote code execution, against the same product and component, and the threat intelligence firm Defused reported exploratory exploitation attempts against its E-Business Suite decoys on 27 October, a week after the patch. Oracle has not confirmed exploitation, and the flaw had not been added to the KEV catalog in the sources we checked, but it echoes the sequence seen with CVE-2026-46817 earlier this year, which was exploited

roughly six weeks after its patch. No new entry this month touches Oracle Payments, but CVE-2026-46817, fixed in May and on the KEV catalog since 15 July, should still be confirmed as patched. Any E-Business Suite estate that has not independently confirmed the October CPU should treat that as the priority ahead of this month's new entries.

Oracle PeopleSoft

PeopleSoft receives 13 patches, 6 of them unauthenticated, and its ceiling returns to 9.8 after September's 8.8. Three entries score 9.0 or higher, all unauthenticated over HTTP: CVE-2026-111497 at 9.8 in the OpenSearch Dashboards (Node.js) component, CVE-2026-114934 at 9.3 in Integration Broker, and CVE-2026-114862 at 9.1 in the WebLogic component. Coverage spans PeopleTools 8.61 through 8.63.

The first of these is the one to act on first. CVE-2026-111497 is an out-of-bounds write in the Brotli decoder in Node.js, a third-party component in PeopleTools' OpenSearch Dashboards deployment, and it is the vulnerability CISA added to the KEV catalog on 27 October with a federal remediation date of 10 November. PeopleSoft estates running OpenSearch Dashboards should treat it as an exploited vulnerability rather than a routine 9.8; see the active exploitation section. The matrix also includes CVE-2026-114937 in Updates Environment Management, the component at the centre of the May and June zero days, though at 8.8 and requiring authentication.

As in September, the concern is historical as well as current. PeopleSoft remains under sustained adversary attention following the exploitation of CVE-2026-35273 by the group tracked as UNC6240 and publicly known as ShinyHunters between 27 May and 9 June, and any internet-facing instance that was unpatched during that window warrants a compromise investigation regardless of its current patch level.

Oracle Java SE

Java SE receives 11 patches this month, up from 3 in September, and Oracle rates all 11 as remotely exploitable without authentication. September's three entries were confined to the GraalVM Compiler component. This month's span the core JDK release lines, 8u511b33 (including the Java 8 Enterprise Performance Pack build), 11.0.33, 17.0.21, 21.0.13, 25.0.5 and 27.0.1, as well as Oracle GraalVM for JDK, GraalVM Enterprise Edition and JavaFX.

The highest Oracle score among the 11 is 8.1 for CVE-2026-114938 in the Compiler component, followed by 7.5 for a libxml2 flaw in JavaFX (CVE-2026-86144), 7.4 for two entries in JGSS and JSSE (CVE-2026-114939 and CVE-2026-114940), and 7.0 for two further entries in Compiler and Libraries. On Oracle's CVSS 3.1 scoring, none reaches the critical band, and that reading understates the first of them. CVE-2026-114938 is Java4Shell, discussed in the next section, and its score reflects a high attack complexity rating rather than any limit on what a successful attacker obtains, which Oracle rates as high for confidentiality, integrity and availability.

Oracle also issued two out-of-cycle Java updates in October: a Security Alert on 21 October for CVE-2026-91403, a 9.1 in the JSSE component affecting Java SE and GraalVM, and one on 24 October for CVE-2026-114820, which removes a set of impacted eMudhra root CA certificates and reappears this month at 9.1 in the Communications matrix for products that embed Java. Customers should confirm that both alerts, the October CPU and the November CSPU have been applied to every Java runtime, including those bundled inside third-party applications. The structural point from prior CSPUs is unchanged and this month is literal: Fusion Middleware, WebLogic, Hyperion, PeopleTools and E-Business Suite all execute on the Java Virtual Machine, so a flaw in the runtime itself sits beneath all of them.

Other families of note

Supply Chain receives 74 patches, 36 of them unauthenticated, 43 in Oracle AutoVue. AutoVue carries CVE-2026-114980 at 9.9, which requires authentication, and four unauthenticated 9.8s in its Security component (CVE-2026-127324 through CVE-2026-127327). Agile PLM adds an unauthenticated 9.1 in its File Manager component, an Apache Tomcat flaw over HTTP/2 (CVE-2026-101356).

Database Server has 7 patches, 3 unauthenticated, but its ceiling rises to 9.9 on three entries over Oracle Net that require authentication: CVE-2026-114819 and CVE-2026-114848 in Oracle Text and CVE-2026-114822 in the RDBMS. Oracle APEX (2 patches, both unauthenticated 9.8s over HTTPS, CVE-2026-114849 and CVE-2026-114850) and REST Data Services (8 patches, 5 unauthenticated, with a 9.8 and a 9.6) add to the database-adjacent exposure. Communications (31 patches, 21 unauthenticated) carries the KEV-listed Brotli and Node.js flaw in Diameter Signaling Router and Unified Assurance, plus further bundled third-party 9.8s in Unified Assurance's Core component, CVE-2026-1229 and CVE-2026-41889. MySQL appears this month with 10 patches, including a 9.8 in MySQL Shell's Core Client (CVE-2026-115557). Siebel CRM falls to 19 patches with a ceiling of 8.8, and Virtualization to 11 with a ceiling of 8.6.

Java4Shell (CVE-2026-114938)

On 17 November, the security research firm Calif.io disclosed Java4Shell, tracked as CVE-2026-114938, a memory corruption vulnerability in the Base64 decoder that OpenJDK's HotSpot virtual machine uses on x86-64 processors. Oracle credits Calif.io's Quang Luong and Albert Yang in the CSPU's credit statement and lists the flaw in the Java SE risk matrix against the Compiler component, consistent with Calif's description of a flaw in a C2 compiler intrinsic. CISA published an alert the same day strongly urging organizations to patch immediately. Oracle scores the flaw 8.1 under CVSS 3.1 (network, high attack complexity, no privileges, no user interaction, high impact on confidentiality, integrity and availability). Calif scores it 9.2 under CVSS 4.0.

The bug is in hand-written assembly that accelerates Base64 decoding on processors with AVX-512 VBMI. When the padded tail of the input should produce zero output bytes, a length calculation underflows, and a masked 64-byte store then writes past the end of the output array. A trigger as small as 64 "A" characters followed by a single "=" (128 on older JDK 17 builds) corrupts neighboring heap objects before Java rejects the input as invalid. Base64 is ordinary plumbing for authentication tokens, file uploads and network messages, so an application does not need to do anything unusual to expose the decoder.

Calif reports that the overwrite can be turned into a Heartbleed-style disclosure of heap contents, which can hold tokens, keys and personal data, and into remote code execution. It demonstrated unauthenticated code execution against Keycloak, Jira, Confluence, Artifactory, Jenkins and PingFederate in default configurations, authenticated code execution against Kafka, Solr, Elasticsearch, Gerrit and Spinnaker, and sample applications built on Spring Boot and Apache Struts. It also describes a client-side route in which a Java program that opens a TLS connection to a malicious server can be compromised. Calif is withholding the product-specific exploit chains and says there is no universal exploit: each target needs its own heap-grooming profile, attacks are sensitive to network latency, and a failed attempt can crash the JVM, though it can often be retried. A bounded proof of concept that demonstrates the overwrite is public.

Exposure requires three conditions: an affected build, an x86-64 processor with AVX-512 VBMI (Intel Xeon from Ice Lake onward, AMD EPYC and Ryzen from Zen 4 onward; ARM64 is not affected), and attacker-controlled Base64 data reaching the decoder. Oracle lists Java SE 8u511b33-perf, 17.0.21.0.3, 21.0.13.0.3, 25.0.5.0.3 and 27.0.1.0.3, Oracle GraalVM for JDK 17.0.21.0.3 and 21.0.13.0.3, and GraalVM Enterprise Edition 21.3.20.0.3. Calif reports that OpenJDK from 17.0.6 onward is affected, so distributions built from it, including Amazon Corretto, Eclipse Temurin, Microsoft Build of OpenJDK, Azul Zulu, BellSoft Liberica, SAP SapMachine and Red Hat builds, are in scope as well. Many enterprise products bundle their own JDK, which operating system updates will not patch.

As of publication, no exploitation in the wild has been publicly reported and the flaw is not on the CISA KEV catalog. That describes the first day, not the outlook. The root cause and trigger are public, and Calif reports that it found the bug in about an hour using an AI coding agent, built the first working exploit in two further hours, and spent under $200 in compute. The same tooling is available to attackers, which shortens the interval between a patch and a working exploit. Recommended actions:

1. **Inventory every Java runtime**, including those bundled with third-party applications and embedded in container images, and identify hosts whose CPUs support AVX-512 VBMI. On Linux, check `/proc/cpuinfo` for the `avx512f`, `avx512bw`, `avx512vbmi` and `bmi2` flags.
2. **Apply Oracle's November Java updates**, or the equivalent fixed build from your distribution, and restart each JVM, since a patched package does not protect a process that is still running. Oracle's Java SE patch availability document on My Oracle Support is the authoritative source for the fixed build numbers.
3. **Where patching must wait**, Calif recommends the following flags:
   - Disable the Base64 intrinsics with `-XX:-UseBASE64Intrinsics`. Expect some performance cost on workloads that perform a lot of Base64 encoding or decoding operations.
   - Cap vector instructions at AVX2 with `-XX:UseAVX=2`. This flag only exists on x86-64 builds, and an ARM JVM will refuse to launch if it's present.
   - Avoid adding `-XX:DisableIntrinsic=_base64_decodeBlock` by itself. It is a diagnostic option, so the JVM won't start unless `-XX:+UnlockDiagnosticVMOptions` comes before it. Rolling it out across a fleet of JVMs can cause a massive outage.

   Neither replaces the patch, and buffering requests at a reverse proxy is not a dependable mitigation.
4. **Prioritize internet-facing identity services** such as Keycloak and PingFederate, which decode attacker-supplied Base64 (Basic auth client credentials, JWTs, SAML requests), then internet-facing Jenkins, Artifactory, Jira and Confluence, then other Java services that decode tokens, credentials or uploads.

Vulnerabilities under active exploitation

One vulnerability patched in the November CSPU is confirmed exploited, and it is a third-party flaw rather than an Oracle-originated one. No other vulnerability first disclosed in this release, including Java4Shell, has been publicly confirmed as exploited as of publication. Several previously disclosed flaws in products covered by this release also remain part of the practical threat picture.

CVE-2026-111497, Google Brotli decoder (Node.js), PeopleSoft and Oracle Communications, CVSS 9.8

An out-of-bounds write in the Brotli decoder, affecting Google Brotli 1.0.3 through 1.2.0 and the Node.js releases that embed it, that lets a remote, unauthenticated attacker corrupt memory with a crafted Brotli stream and can lead to a crash, information disclosure or remote code execution. Oracle's November matrices list it three times, each at 9.8 and unauthenticated over HTTP: the OpenSearch Dashboards (Node.js) component of PeopleSoft PeopleTools, the PMAC (Node.js) component of Communications Diameter Signaling Router, and the Core (Brotli) component of Communications Unified Assurance. Upstream fixes shipped on 21 October, exploitation attempts followed within days, and CISA added the CVE to the KEV catalog on 27 October with a federal remediation date of 10 November, a week before Oracle's fix arrived. Any PeopleSoft or Communications deployment that has not applied this CSPU should be treated as exposed to a KEV-listed vulnerability.

CVE-2026-101767, Oracle E-Business Suite, Application Object Library, CVSS 9.8

An unauthenticated SQL injection that can chain to remote code execution, fixed in the October 2026 CPU and affecting versions 12.2.3 through 12.2.15. Defused recorded exploratory exploitation attempts against its E-Business Suite decoys on 27 October. Oracle has not confirmed exploitation in the wild, and the CVE had not been added to the KEV catalog in the sources we checked, but any estate that has not applied the October CPU should treat it as under attack.

CVE-2026-109618 and CVE-2026-109619 (PHP2Shell), Oracle Communications and other products, CVSS 9.8

Two PHP vulnerabilities, also found by Calif.io, that allow unauthenticated remote code execution. Oracle issued a Security Alert on 25 October covering affected products that include Communications Diameter Signaling Router, EAGLE and Performance Intelligence Center, and Secure Backup. Working remote code execution was observed against honeypots within days, and CISA has added both CVEs to the KEV catalog.

Carried forward from earlier CSPUs

The four flaws highlighted in September remain exploited and their status is unchanged: CVE-2026-21962 in the WebLogic Server Proxy Plug-in (KEV, 24 August), CVE-2026-35273 and CVE-2026-35278 in PeopleSoft PeopleTools (exploited as zero days by ShinyHunters from 27 May to 9 June), and CVE-2026-46817 in Oracle Payments (KEV, 15 July). Verifying their remediation still comes ahead of this month's new patches.

The pattern is consistent across all of these. Exploitation arrives within days of a disclosure or a patch, often once proof-of-concept code is public, and in the Brotli case the federal deadline had already passed by the time Oracle's fix shipped. A patch that exists but has not cleared regression testing provides no protection, and neither does one applied to a system that was already compromised during the exposure window.

Waratek recommends a defense-in-depth posture for these attack chains, so that there are multiple points at which an attack can be intercepted rather than a single dependency on patch availability and deployment speed. Waratek customers who need assistance identifying or enabling the relevant controls should contact our Customer Success team.

How Waratek addresses the risk

Waratek RASP operates inside the Java Virtual Machine rather than at the network perimeter. Because it enforces on what the application is actually doing at runtime, it addresses classes of unsafe behavior including deserialization of untrusted data, server-side request forgery, path traversal, command injection, JNDI and LDAP lookups, SQL injection and XML external entity processing, independent of which specific CVE number is behind the behavior.

That distinction matters for how this month's disclosures arrived. Calif's account of Java4Shell, a bug found in about an hour with an AI coding agent and weaponized in two more for under $200, shows how quickly discovery, triage and exploit development are becoming cheaper for attackers as well as defenders. Coverage organized around behavior, rather than around a specific CVE identifier, applies equally to a vulnerability and automated pipeline surfaced last month, one a human researcher reports tomorrow, and one that has not been disclosed to anyone yet.

Java4Shell needs a precise statement. The flaw sits in HotSpot's native code rather than in application code, so the primary remediation is the Oracle update or the JVM flag described above, and runtime rules are not a substitute for either. What runtime protection contributes is constraining what an attacker can do with the foothold the flaw provides.

Waratek's hardening rules (file, network and process) constrain what an attacker can do from inside a protected JVM. With the hardening rules enabled, specific actions are blocked, such as spawning OS processes, writing executable files and opening unexpected outbound connections. That limits the post-exploitation activity attackers typically rely on after compromising a Java service.

Preemptive Security rules and patching together supply the one thing the current release cadence removes, which is time. Waratek applies compensating controls with no source code changes, no recompilation and no downtime, so exposure can be reduced the day an advisory lands while regression testing and vendor patching proceed on a schedule the business can absorb.

That is directly relevant to Fusion Middleware and Hyperion estates carrying this month's unauthenticated 10.0 and 9.8 findings, to PeopleSoft and Communications environments exposed to the KEV-listed Brotli flaw, to E-Business Suite environments where the October CPU may not yet be applied, and to every Java estate now rolling out Java4Shell updates.

Waratek customers should contact our Customer Success team for guidance on which existing RASP rules already cover the vulnerability classes represented in the November 2026 CSPU.

Frequently asked questions

Is anything in this release under active exploitation right now?

One item is. CVE-2026-111497, the Brotli decoder flaw in Node.js, is on the CISA KEV catalog and appears in the PeopleSoft PeopleTools, Communications Diameter Signaling Router and Communications Unified Assurance entries. Nothing else first disclosed in the CSPU, including Java4Shell, has been publicly confirmed as exploited as of publication. Exploitation is also confirmed for the PHP2Shell flaws addressed by October's Security Alert, CVE-2026-21962 in WebLogic, CVE-2026-35273 and CVE-2026-35278 in PeopleSoft and CVE-2026-46817 in Oracle Payments, and exploratory attacks against CVE-2026-101767 in E-Business Suite have been recorded. Verify these before turning to this month's new patches.

How serious is Java4Shell if Oracle scores it only 8.1?

Treat it as urgent for exposed systems. Oracle's 8.1 reflects a high attack complexity rating, not a limit on impact. Calif scores it 9.2 under CVSS 4.0 and has demonstrated unauthenticated remote code execution against several widely used Java products, and CISA has urged immediate patching. The mitigating factors are real: exploitation needs an x86-64 CPU with AVX-512 VBMI, attacker-controlled Base64 reaching the decoder, and a bespoke chain per application. Prioritize internet-facing Java services on affected hardware, patch or apply the JVM flag, and do not wait for exploitation reports.

Does Java4Shell affect us if we run Java 8 or Java 11, or run on ARM?

Oracle's list names only one Java 8 build for this CVE, the Enterprise Performance Pack build 8u511b33-perf, and does not list Java 11, so standard Java 8 and Java 11 builds appear unaffected. Oracle's list does include 17, 21, 25 and 27 and the GraalVM builds above, and Calif reports that OpenJDK from 17.0.6 onward is affected. ARM64 systems and x86-64 CPUs without AVX-512 VBMI are not affected. Confirm against Oracle's patch availability document and your distribution's advisory, and remember that bundled JDKs inside third-party products need their own update.

Should we prioritize the six 10.0 issues first?

Prioritize by exposure and exploitation status first, and by score second. Verify remediation of the exploited vulnerabilities above, apply the Java updates to internet-facing runtimes, then take the six maximum-severity findings on anything externally reachable: five in Fusion Middleware, spanning Access Manager, Platform Security for Java and WebLogic Server, plus one in Business Intelligence Enterprise Edition. All six require no authentication. From there, move to the unauthenticated 9.8s in Hyperion, WebLogic's Core component over T3 and IIOP, and the E-Business Suite Application Object Library.

Is PeopleSoft urgent this month?

Yes, for one specific reason. Its highest entry, CVE-2026-111497, is the KEV-listed Brotli and Node.js flaw in the OpenSearch Dashboards component, so any PeopleTools deployment that uses it should be treated as exposed until patched. Beyond that, the release is modest at 13 patches, but PeopleSoft remains under sustained, named adversary attention independent of this release, so confirming coverage of the May and June zero days still matters.

We cannot regression test 655 patches within the monthly window. What are our options?

Prioritize internet-facing and unauthenticated attack surface first, since 303 of the 655 patches address issues exploitable with no credentials, and put Java runtime updates and the KEV-listed Brotli flaw at the front of the queue. Establish compensating controls, such as a runtime rule or, for Java4Shell, the JVM flag, for what cannot be patched immediately so the exposure window is covered while testing proceeds. Runtime protection is designed for exactly this gap, reducing risk on day one without a code change or an outage.

For more information

Waratek customers should contact customersuccess@waratek.com for guidance on which RASP rules already cover CVEs in the November 2026 CSPU.

Prospects evaluating Waratek can contact sales@waratek.com for a protection assessment.

Source advisory: oracle.com/security-alerts/cspunov2026.html

Java4Shell research (Calif.io): calif.io/java4shell

CISA alert: cisa.gov/news-events/alerts/2026/11/17/critical-java-vulnerability-requires-immediate-patching

This bulletin is a security news summary compiled by Waratek for customers and prospects from Oracle's published Critical Security Patch Update Advisory for November 2026 and its risk matrices, from the Calif.io disclosure of Java4Shell, and from public reporting on active exploitation. It is not an official Oracle publication. All Oracle product names are trademarks of Oracle.