Projektzusammenfassung

vtdr-v1.0 und KRITIS 3.0 — Schwachstellen-Forschung für WordPress

Stand: 24. Juni 2026 · Träger: VTDR i. G. · Version 1.1.0

Worum geht es?

Das Projekt untersucht systematisch Sicherheitslücken in WordPress — dem weltweit meistgenutzten System zum Betrieb von Webseiten. Im Mittelpunkt stehen die unzähligen Erweiterungen (sogenannte Plugins und Themes), die Webseiten um Funktionen erweitern und erfahrungsgemäß die häufigste Quelle für angreifbare Schwachstellen sind.

Ziel ist es, diese Schwachstellen nicht nur theoretisch zu beschreiben, sondern in einer abgeschotteten Testumgebung praktisch und beweissicher nachzuweisen. Die Ergebnisse sind so aufbereitet, dass sie an Sicherheitsbehörden wie das BSI (Bundesamt für Sicherheit in der Informationstechnik) und CERT-Bund übergeben werden können, damit betroffene Betreiber rechtzeitig gewarnt und Hersteller zur Behebung aufgefordert werden.

Sämtliche Tests laufen ausschließlich gegen eigene, lokale Testsysteme — niemals gegen fremde Webseiten. Das Projekt bewegt sich damit im rechtlich zulässigen Rahmen (§ 202c StGB).

Die wichtigsten Zahlen auf einen Blick

Kennzahl	Wert
Nachgebaute, beweissichere Exploits insgesamt	1.230
Davon zu bekannten, veröffentlichten Schwachstellen (CVEs)	971
Selbst neu entdeckte Schwachstellen (0-Days)	202
Betroffene Plugins/Themes mit eigenen 0-Day-Funden	184
Davon kritischer Schweregrad (CVSS ≥ 9,0)	30
Davon hoher Schweregrad (CVSS 7,0–8,9)	96
Erfolgsquote im letzten Massentest	ca. 93 %
Reproduzierbarkeit der Nachweise	20 von 20 (100 %)

Das Projekt besteht aus zwei Teilen

Die Arbeit stützt sich auf zwei Werkzeuge, die zusammenspielen — das eine sucht, das andere weist nach:

1. KRITIS 3.0 — der passive Suchscanner

KRITIS 3.0 durchsucht Webseiten schonend von außen, ohne sie anzugreifen oder zu verändern. Es erkennt, welche WordPress-Version und welche Plugins in welcher Version eingesetzt werden, und gleicht das mit bekannten Schwachstellen-Datenbanken ab. So entsteht eine priorisierte Liste verdächtiger Kandidaten. Das Verfahren ist datenschutzkonform (Art. 32 DSGVO) und liefert einen gutachtenartigen Bericht (PDF).

2. vtdr-v1.0 — der aktive Nachweis

vtdr-v1.0 nimmt die Kandidaten und weist die Schwachstelle in einer abgeschotteten Testumgebung tatsächlich nach. Für jede Lücke entsteht ein lückenloses Protokoll des Angriffs (eine sogenannte HAR-Datei) plus eine verständliche Beweisdokumentation. Ein Prüfer beim BSI kann damit den Nachweis Schritt für Schritt selbst nachstellen.

Schwerpunkt: 202 selbst entdeckte 0-Day-Schwachstellen

Ein „0-Day“ ist eine bisher unbekannte Sicherheitslücke — sie ist weder öffentlich gemeldet noch vom Hersteller behoben. Der Name kommt daher, dass der Hersteller „null Tage“ Zeit hatte, sie zu schließen. 0-Days sind besonders wertvoll und besonders gefährlich, weil Angreifer sie ausnutzen können, solange noch kein Schutz existiert.

Im Rahmen des Projekts wurden 202 solcher bislang unbekannter Schwachstellen neu entdeckt und beweissicher nachgewiesen. Sie verteilen sich auf 184 verschiedene Plugins und Themes.

Hinweis zur Zählweise: Maßgeblich sind die 202 eigenständig dokumentierten 0-Day-Funde. Einige davon haben inzwischen im Zuge der Meldung eine offizielle CVE-Nummer erhalten, behalten aber ihre ursprüngliche 0-Day-Kennung.

0-Days nach Schweregrad (CVSS)

Der CVSS-Wert misst auf einer Skala von 0 bis 10, wie gefährlich eine Schwachstelle ist. Je höher, desto kritischer:

Schweregrad	CVSS-Bereich	Anzahl 0-Days
Kritisch	9,0 – 10,0	30
Hoch	7,0 – 8,9	96
Mittel	4,0 – 6,9	74
(noch ohne Bewertung)	—	2
Summe		202

Bemerkenswert: 126 der 202 Funde (rund 62 %) sind hoch oder kritisch eingestuft — sie können also ernsten Schaden anrichten.

0-Days nach Art der Schwachstelle

Die entdeckten Lücken verteilen sich auf folgende Angriffsarten:

Art der Schwachstelle (vereinfacht)	Anzahl
Umgehung von Zugriffsrechten (Broken Access Control)	111
Ungewollte Preisgabe von Informationen	23
Umgehung der Anmeldung (Auth-Bypass)	17
Zugriff auf fremde Daten (IDOR)	15
Einschleusen von Datenbankbefehlen (SQL-Injection)	8
Hochladen schädlicher Dateien	8
Ausweitung von Benutzerrechten (Privilege Escalation)	7
Server-seitige Anfragefälschung (SSRF)	6
Schädlicher Code im Browser (XSS)	3
Sonstige (RCE, LFI, Code-Injection, schwache Kryptografie)	4

Der mit Abstand häufigste Fund — die Umgehung von Zugriffsrechten — bedeutet, dass Funktionen oder Daten erreichbar waren, die eigentlich geschützt sein sollten. Das ist eine der klassischen und folgenreichsten Schwachstellen in Web-Anwendungen.

971 nachgebaute Exploits zu bekannten Schwachstellen

Neben den eigenen Funden wurden 971 bereits öffentlich bekannte Schwachstellen (CVEs) praktisch nachgebaut und verifiziert. Das dient zwei Zwecken: Erstens wird belegt, dass eine gemeldete Lücke tatsächlich ausnutzbar ist (und nicht nur auf dem Papier existiert). Zweitens lernt das System aus jedem Nachbau und wird beim Aufspüren neuer 0-Days immer treffsicherer.

Zusammen mit den 0-Day-Funden ergibt das einen Bestand von insgesamt 1.230 vollständig dokumentierten, beweissicheren Exploits.

Verteilung aller Exploits nach Schwachstellen-Art

Art der Schwachstelle	Anzahl
SQL-Injection (Datenbankbefehle einschleusen)	302
Broken Access Control (Rechte-Umgehung)	272
Datei-Upload-Lücken	123
Privilege Escalation (Rechte-Ausweitung)	89
Auth-Bypass (Anmeldung umgehen)	81
Cross-Site-Scripting (XSS)	79
Local File Inclusion (LFI)	75
Informations-Preisgabe	55
Remote Code Execution (RCE)	34
Server-Side Request Forgery (SSRF)	33
Weitere (Code-Injection, IDOR, Deserialisierung, CSRF u. a.)	87

Wie zuverlässig sind die Ergebnisse?

Beweissicherheit ist die oberste Priorität des Projekts. Damit ein Nachweis anerkannt wird, muss er von einer dritten Stelle exakt nachstellbar sein. Dafür sorgen mehrere Mechanismen:

- **Lückenlose Protokollierung:** Jeder einzelne Angriffsschritt wird mitprotokolliert und ist im Beweispaket sichtbar — nichts wird simuliert oder nachträglich verändert.
- **Automatischer Wächter:** Eine automatische Prüfinstanz kontrolliert jeden Exploit anhand von 48 festen Regeln auf Manipulation und Beweiskraft, bevor er als gültig zählt.
- **Reproduzierbarkeit:** Stichproben werden mehrfach wiederholt — zuletzt mit einem perfekten Ergebnis von 20 aus 20 identischen Durchläufen (100 %).
- **Massentests:** In regelmäßigen Massentests werden alle Exploits erneut gegen die Testumgebung gefahren. Der jüngste Lauf erreichte rund 93 % bestätigte Treffer.

Die Testumgebung ist auf eine exakte Software-Version festgenagelt, sodass jeder Nachweis Jahre später unter identischen Bedingungen wiederholbar bleibt.

Reichweite der Erfassung (KRITIS 3.0)

Um Kandidaten für die Nachweise zu finden, wurden große Mengen an Webseiten schonend gescannt. Ein einzelner Durchlauf erfasste beispielhaft:

Kennzahl des Scan-Laufs	Wert
Geprüfte Webseiten (Domains)	8.767
Erfolgreich ausgewertet	7.413
Mit Treffer auf bekannte Schwachstellen	5.713
Korrektheit der Plugin-Erkennung	100 %
Fehlalarmrate des Schadcode-Scanners	0 %
Parallele anonymisierte Scan-Kanäle (Tor)	45

Die Erkennung wurde über mehr als 6.000 Berichte kalibriert und liefert dadurch verlässliche, fehlalarmarme Ergebnisse.

Fazit

Das Projekt verbindet zwei Stärken: das großflächige, schonende Aufspüren verdächtiger WordPress-Installationen und den anschließenden, gerichtsfest aufbereiteten Nachweis der Schwachstelle. Das Kernergebnis sind 202 eigenständig neu entdeckte 0-Day-Schwachstellen — davon 30 als kritisch und 96 als hoch eingestuft — sowie insgesamt 1.230 beweissichere Exploits.

Damit liefert das Projekt einen unmittelbaren Sicherheitsgewinn: Hersteller können ihre Produkte korrigieren und Sicherheitsbehörden betroffene Betreiber frühzeitig warnen, bevor die Lücken durch Angreifer ausgenutzt werden.

Dieses Dokument fasst den technischen Projektstand allgemeinverständlich zusammen. Die vollständige technische Dokumentation befindet sich im Verzeichnis DOKU/ des Projekts.