

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- ▼ [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Vulnerabilities](#)



Access Bypass, Data Overwrite Vulnerabilities Patched in Drupal

By [Ionut Arghire](#) on April 21, 2022

Share

发推

推荐 13



Drupal on Wednesday announced the release of security updates to resolve a couple vulnerabilities that could lead to access bypass and data overwrite.

The first of the bugs fixed with the latest iterations of the open source content management system (CMS) is an access bypass issue that exists because of an improperly implemented generic entity access API for entity revisions.

“This API was not completely integrated with existing permissions, resulting in some possible access bypass for users who have access to use revisions of content generally, but who do not have access to individual items of node and media content,” Drupal [explains](#).

The vulnerability impacts Drupal 9.3 versions only, and solely affects sites where Drupal's revision system is in use.

[**READ:** [Oracle Releases 520 New Security Patches With April 2022 CPU](#)]

The second issue was identified in the Drupal core's form API and is described as an improper input validation in certain contributed or custom modules' forms.

Due to [this security hole](#), an attacker could inject disallowed values or overwrite data. The affected forms are uncommon, but Drupal notes that, in certain cases, the flaws could allow an attacker to modify critical or sensitive data.

“We do not know of affected forms within core itself, but contributed and custom project forms could be affected,” Drupal says.

Both of these vulnerabilities are rated “moderately critical” and users are advised to update to a patched version as soon as possible.

The bugs were resolved with the release of Drupal 9.3.12 and Drupal 9.2.18. Drupal 9 versions prior to 9.2.x and Drupal 8 have reached end-of-life (EOL) status and will not be updated. Drupal 7 is not impacted.

Related: [Juniper Networks Patches Vulnerabilities in Contrail Networking, Junos OS](#)

Related: [Several Access Bypass, CSRF Vulnerabilities Patched in Drupal](#)

Related: [Citrix Patches Vulnerabilities in Several Products](#)

[Share](#)[发推](#)[推荐 13](#)[RSS](#)

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[Meta Offers Rewards for Flaws Allowing Attackers to Bypass Integrity Checks](#)

[Access Bypass, Data Overwrite Vulnerabilities Patched in Drupal](#)

[Cisco Patches Virtual Conference Software Vulnerability Reported by NSA](#)

[FBI Shares Information on BlackCat Ransomware Attacks](#)

[New BotenaGo Variant Infects Lilin Security Cameras With Mirai](#)

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

sponsored links

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

[2022 Singapore/APAC ICS Cyber Security Conference\]](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

Tags:

[NEWS & INDUSTRY](#) [Vulnerabilities](#)

Get the Daily Briefing

BRIEFING

