Ø Ø COVERED

Community

Number one vulnerability management and threat intelligence platform documenting and explaining vulnerabilities since 1970.

VulDB CTI Team identified activities by APT actor "United States of America"

VulDB Mod Team queued 10 new entries

VulDB Data Team updated 33 entries

VulDB Mod Team merged 2 submitted duplicates

Jamesling joined the community

Vulnerability of the Day

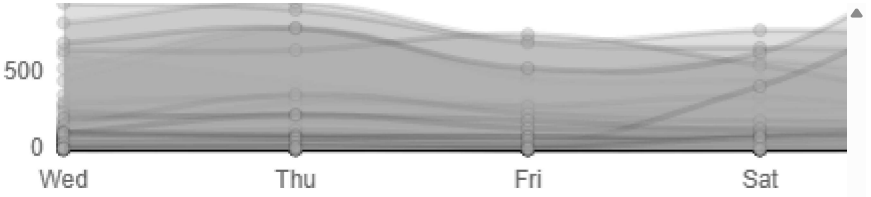
VMware Spring Cloud Gateway Header

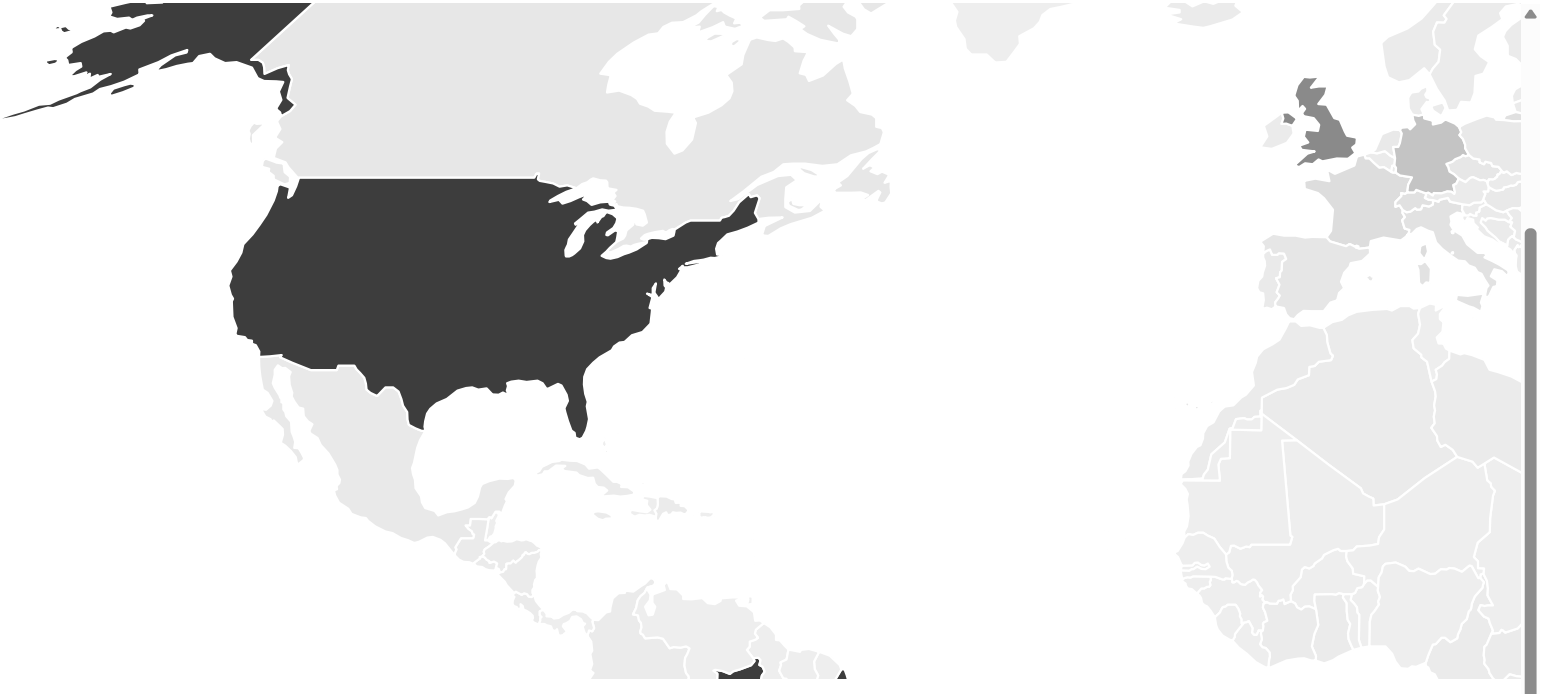
A vulnerability has been found in **VMware Spring Cloud Gateway and Spring Cl Gateway Server MVC** and classified as **problematic.** This vulnerability affects unkn code of the component *Header Handler*. The manipulation of the argument *X-Forwar For/Forwarded* leads to an unknown weakness. This vulnerability was named **CVE-2(41235.** The attack can be initiated remotely. There is no exploit available. It recommended to upgrade the affected component.

Find more vulnerabilities...

Threat Intelligence

3.22	**Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 ssid1MACFilter os...**
2.99	chaitak-gorai Blogbook GET Parameter post.php sql injection
2.93	fossasia open-event-server Mail Verification mail.py send_email_change_user_...





Recent

The moderation team is monitoring different sources 24/7 for the disclosure of information about new or existing vulnerabilitities. If a new issue is determined, additional data from ot sources is collected and a new VulDB entry created. This entry is then pushed to customers, the web site and accessible via API and social media accounts. Please use the **submit feat** to suggest new sources and entries.

click5 History Log Plugin cross site scripting

Updates

If the moderation team detects changes of existing vulnerabilities or new data of existing vulnerabilities are getting published, the old entries will be updated. This happens if needed on a regular basis which concludes in a maximum of data quality. Every entry contains a timestamp of the last update and a change log of updated fields. Please use the edit featur commit updates to existing entries.

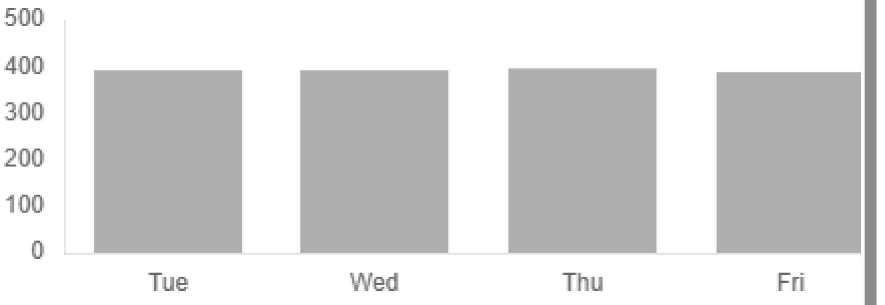
Splunk Universal Forwarder SplunkUniversalForwarder permission assignment

xls2csv Shared String Table Record Parser integer overflow to buffer overflow

Dreamstime Stock Photos Plugin cross site scripting

Cimatti Consulting Contact Forms Plugin cross-site request forgery

ConnectWise ScreenConnect ASP.NET Web Forms code injection



CVSS Current Top

Top vulnerabilities with the highest **CVSSv3 temp scores** at the moment. The score is generated by separate values which are called vectors. Those vectors define the structure of vulnerability. They rely on attack prerequisites and impact. The calculated score ranges between 0.0 and 10.0 whereas a high value declares a high risk. The main score is the base sc which analyses the structure of the vulnerability only. The extended score called temp score introduces time-based aspects like exploit and countermeasure availability. Our moderat classify every entry to generate a CVSS score as accurate as posible.

9.8 Evertz SVDN 3080ipx-10G Web Management Interface command injection

Exploit Price Current Top

Top vulnerabilities with the highest **exploit price** at the moment. These price estimations are calculated prices based on mathematical algorithm. This algorithm got developed by specialists over the years by observing the exploit market structure and exchange behavior of involved actors. It allows the prediction of generic prices by considering multiple techn aspects of the affected vulnerability. The more technical details are available the higher the accuracy of the reproducable approximation.

$10k-$25k	Apple iOS/iPadOS cross-domain policy
$10k-$25k	Google Chrome libvpx use after free
$10k-$25k	Google Chrome V8 out-of-bounds write
$10k-$25k	Google Chrome Compositing use after free
$10k-$25k	Google Chrome Messages ui layer