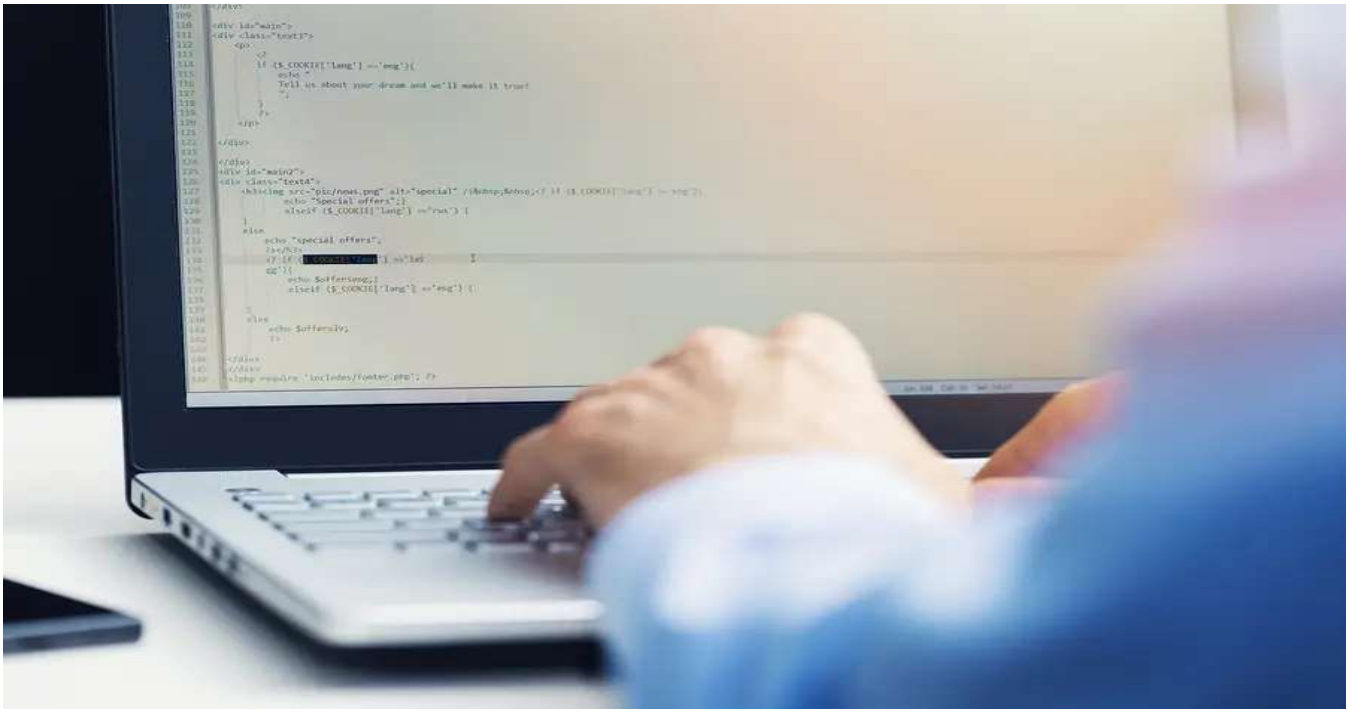
The Telltale Text File: Security Researcher Proposes Standardization for Reporting Vulnerabilities



| September 19, 2017

By Douglas Bonderud | 2 min read

Share

Web security solutions lack standardization for reporting vulnerabilities. Security researcher Ed Foudil recently submitted a draft to the Internet Engineeing Task Force (IETF) that suggested creating a standardized security.txt file on every website that details the site's security policy and provides contact information to report new vulnerabilities.

The Dangers of Delayed Response

in D-Link routers and reported them all to the company. Despite months of back and forth, Embedi said only one of the vulnerabilities was patched.

The firm also contacted the Community Emergency Response Team (CERT) and was told to use D-Link's official reporting channels. In August, the security firm released exploit code for all three vulnerabilities since there was no evidence of further patch progress.

This isn't the ideal route for security professionals and security firms. They would prefer to work with developers, create a patch and then release code into the wild, especially since cybercriminals start working on new attack variations within hours after any new weakness is made public.

Lacking standardization, white-hat hackers are forced to wait on corporate responses. Often there is no viable way to contact organizations directly, leaving researchers with the difficult choice of keeping quiet and hoping no one else notices the issue or speaking up to compel change, risking exploitation by malicious actors.

A New Standard for Reporting Vulnerabilities

As noted by Bleeping Computer, Foudil got his idea after attending DEF CON this year. He modeled his new security.txt after robots.txt, which is used by web search spiders when they index sites. Standardization of robots.txt has significantly improved the efficiency of this indexing, and Foudil imagined something similar for the security.txt protocol. In his version, however, the file is kept on the top level of company web servers and read by human beings.

The current draft supports four directives: contact, encryption, disclosure and acknowledgment, which would give security researchers the information they need to make contact and start the process of remediating code flaws. So far, security.txt has been met with support from HackerOne, Bugcrowd and Google. If widely adopted, the new .txt file could also be expanded to include directives such as rate-limit, platform, reward, donate and disallow, providing even more specific direction to security firms and researchers.

application patching won't work in a tech landscape characterized by cybercriminals able to pounce on vulnerabilities within hours and companies willing to discount potential defense disasters until it's too late. By creating a simple, standardized format, corporations can provide a direct line for feedback, fraudsters are left out of the loop and security experts can do what they do best: discover and report critical code vulnerabilities.

Application Security | Exploit | Exploit Mitigations | Security Research | Vulnerabilities | Vulnerability Management

Douglas Bonderud

Freelance Writer

A freelance writer for three years, Doug Bonderud is a Western Canadian with expertise in the fields of technology and innovation. In addition to working for...

POPULAR

INTELLIGENCE & ANALYTICS | December 13, 2022

Cybersecurity Trends: IBM's Predictions for 2023

INTELLIGENCE & ANALYTICS | December 29, 2022

The 13 Costliest Cyberattacks of 2022: Looking Back

GOVERNMENT | January 3, 2023

How Can the White House's New IoT Labels Improve Security?

MORE FROM

GOVERNMENT | January 6, 2023

California v. Congress: Data Protection Law Showdown

ENDPOINT | January 5, 2023

3 Reasons to Make EDR Part of Your Incident Response Plan

NEWS | January 4, 2023

New Federal Cybersecurity Requirements for Railway Operators