Our vulnerability disclosure program - established in 2007

SecuriTeam Secure Disclosure (SSD) helps security researchers turn their skills in uncovering security vulnerabilities into a career.

Designed by researchers, for researchers, SSD provides the fast response and support needed to get zero-day vulnerabilities responsibly reported to vendors and to get researchers the compensation they deserve. We help researchers get to the bottom of vulnerabilities affecting major operating systems, software or devices.

Would you like to find out more? Email us at: ssd@beyondsecurity.com.

Scope Submission process Q & A Community Report template

Scope

Targets of interest:

- **Operating systems:** Windows / Linux / OSX
- **Mobile:** iOS / Android
- **Web Browsers:** ToR / Chrome / Safari / Edge / FireFox

- **Readers**: Microsoft Office
- **Web Hosting Control Panel**: cPanel / Plesk / DirectAdmin / Webmin / VestaCP / ISPManager / ISPConfig / Aegir
- **Mailserver**: Microsoft Exchange Server / Zimbra / Roundcube / MDaemon / Horde / Exim / Postfix / Dovecot
- **CMS**: WordPress / Joomla / Drupal / vBulletin
- **Embedded**: Mobile Baseband / NAS / Routers / DVR
- **Network Management Systems**: Zabbix / Nagios / PRTG
- **Others**: PHP / .NET / Firewalls / Protocols

Got a vulnerability out of this scope? Send us an email, we can still help: ssd@beyondsecurity.com

Submission process

1. You send us a brief description of the vulnerability.
2. We may follow up with questions.
3. We sign a contract.
4. You send us the vulnerability.
5. Our technical team verifies the vulnerability.
6. We contact the vendor.
7. You get paid.
8. The vulnerability is responsibly disclosed and published.

Q&A

How much can I earn from working with you?

The amount paid depends on two different variables:

- How widespread is the software/hardware? Popular products typically reach higher amounts.
- How critical is the vulnerability? For example, if you find an unauthenticated arbitrary code execution vulnerability, you would be paid substantially more than for a Cross Site Scripting vulnerability.

What if I want to stay anonymous?

Fine by us! A lot of our researchers choose to stay anonymous.

What is your policy regarding privacy and confidentiality of researcher's information?

We take the privacy of researchers very seriously and do not disclose to any third party (including to customers) any personal information about researchers such as names, aliases, email addresses, bank details, or any other personal or confidential information.

What is the difference between SSD and Bug Bounties or other programs?

Financially:

- We pay more than bug bounty programs.
- If a vendor doesn't have a bug bounty program - we are still interested in acquiring the vulnerability and reporting it to the vendor.
- We believe researchers need to get paid for their effort and we are willing to offer higher rewards.

Administratively:

- We will handle all the reporting process.
- We will publish your research and attribute it per your instructions.

How do I submit my questions or research?

Send us an email ssd@beyondsecurity.com - It's that easy!

The SSD community

As part of our vulnerability disclosure program we have established a community of researchers. We believe in long-term investment in this group and we provide the tools, education and knowledge they need to find more vulnerabilities and advanced attack vectors and discover innovative ways to exploit them.

We sponsor researcher's workshops, courses, software licenses, hardware and conference attendance.

We are always looking for new researchers to join our community. That’s why we are promoting our “**Friend Bring Friend**” program. If you refer us a new researcher and he will start working with us on Operating systems / Mobile / Web Browsers – you will get 10,000$ USD / For other vulnerabilities – you will get 1,000$ USD

As another way to support the international community we sponsor security conferences around the world - from Black Hat USA to community conferences such as DefCamp Romania. We publish vulnerability technical information in our blog (blogs.securiteam.com), on Twitter (@SecuriTeam_SSD) and in vendor advisories. We also give lectures and host hacking competitions at international security conferences.

In 2018 we sponsored and some of our researchers attended:

1. OffensiveCon
2. Hack In The Box
3. Zer0con
4. CanSec

Vulnerability report template

Use this template to speed confirmation of your discovery:

1. Vulnerability Title
2. Date of submission
3. Description of Product (from vendor/site)
4. Description of Vulnerability
    - 4.1 Title
    - 4.2 Product
    - 4.3 Version
    - 4.4 Homepage
    - 4.5 Binary Affected
    - 4.6 Binary Version
    - 4.7 Binary MD5
5. Configuration Requirements
6. Vulnerability Requirements
7. Vulnerability Summary Information
    - 7.1 Vulnerability Class
    - 7.2 Affected Versions Tested
    - 7.3 Affected Versions Assumed (explain assumption)
    - 7.4 Unaffected Versions
    - 7.5 Affected Platforms Tested (Windows, Linux, 32bit, 64bit, 10 RS1, 10 RS2, 2016, Ubuntu, etc.)

For more information, email us at: ssd@beyondsecurity.com.