Responsible Disclosure Policy

Improsec A/S

Improsec's goal is to help improve security in widely used IT systems, including hard- and software products, operating systems, (web) applications, firmware, APIs etc.

The work is carried out to the extent that it will not compromise trust nor confidentiality between Improsec and our customers.

When we identify security issues or vulnerabilities in IT systems, security researchers at Improsec follow the following Responsible Disclosure policy:

1) By default, Improsec does not communicate publicly about potential security problems or vulnerabilities until responsible authorities at the supplier/manufacturer:
    a. have been notified (see Appendix) **and**
    b. have had reasonable time (see 2a) to confirm and verify the given issue, **and**
    c. have issued a software update or recommended workaround (e.g. configuration change) to all relevant customers to solve the issue. This should happen within reasonable time (see 2b).

2) Improsec, however, requires that the supplier/manufacturer satisfactorily complies to the following rules:
    a. The reported issues are recognized and verified by the supplier/manufacturer within **5 business days** (from date of reporting), **and**
    b. The recommended/agreed upon security measures are designed, developed, tested and implemented within **90 calendar days** (from date of reporting) or before an agreed deadline (explicitly agreed upon by Improsec in writing), **and**
    c. (optional) the supplier/manufacturer agrees to publicly accredit Improsec for our work after the identified issues have been resolved, e.g. in a newsletter, website, blog post, release notes and/or CVE.

3) Once the supplier/manufacturer has implemented the agreed security measures, Improsec reserves the right to publish (disclose) a full description of the reported security issues or vulnerabilities, and the collaboration with the supplier/manufacturer to solve these, on our website and other media.

4) Should **1** or **2** not be met by the supplier/manufacturer, Improsec reserve the right, no matter the supplier/manufacturer's stance on publication, to publish (disclose) a full description of the reported security issues or vulnerabilities, even though these may not have been corrected at the given time. Improsec will furthermore publish documentation of our communication with the supplier/manufacturer.

Improsec wish to collaborate with the supplier/manufacturer on necessary security measures and will provide free counselling to a limited extent. Our Responsible Disclosure Policy is in place to ensure that the supplier/manufacturer take their clients/users and the confidentiality, integrity and availability of data, applications and systems seriously.

Appendix

Improsec contacts appropriate authorities, even if these are not specified on their website, contact page or informed by support.

If relevant contact information is not available from the mentioned sources, we will call supplier/manufacturer's main number for contact information to relevant authorities.

The initial inquiry from Improsec will contain, as a minimum, the following information:

a) Improsec's Responsible Disclosure Policy
b) Specific deadlines, including:
    a. Date of reporting
    b. Deadline for verification (date of reporting + 5 business days)
    c. Deadline for announcement (date of reporting + up to 90 calendar days)
c) Contact information, including name of security researcher
d) Whether we wish to be accredited for the given vulnerability
e) Product name and affected version(s) which have been tested
f) Vulnerability type (Remote Code Execution, Local Privilege Escalation, Information Disclosure etc.)
g) Classification of criticality and impact using the CVSS score and calculation method
    a. https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator
    b. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
h) Explanation of attack vector, i.e. what is required to exploit the vulnerability
i) Assessment of how easy it is to exploit the vulnerability
j) Clarification of registration of CVE bulletin ID (Mitre)
k) Sufficient technical information for the supplier/manufacturer to verify our findings

References:

- https://cve.mitre.org/cve/researcher_reservation_guidelines
- http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm
- http://www.cisco.com/c/en/us/about/security-center/vendor-vulnerability-policy.html
- https://www.hackerone.com/disclosure-guidelines
- https://security.googleblog.com/2013/05/disclosure-timeline-for-vulnerabilities.html