Responsible Disclosure Policy

CRYPTRON Security GmbH

22. February 2022

1.1 Responsible Disclosure Policy

In computer security, coordinated disclosure of vulnerabilities is important, so the CRYPTRON Security Research Lab has written a policy on this and summarized key points.

1.2 Coordinated disclosure of vulnerabilities

To follow industry best practices, our process of responsibly disclosing critical vulnerabilities is based on Google's vulnerability disclosure policy. https://www.google.com/about/appsecurity

Information security and vulnerability management is not a state, but a process.

Both vendors and researchers must act responsibly. For this reason, CRYPTRON Security Research Lab adheres to a 90-day vulnerability disclosure period. We notify vendors of vulnerabilities immediately and do not publicly disclose details until 90 days have passed (or sooner if the vendor releases a fix). This deadline may vary in the following ways:

- If a deadline expires on a weekend or U.S. holiday, the deadline is postponed until the next business day.
- If a vendor notifies us before the 90-day deadline that a patch will be released on a specific day that is within 14 days of the deadline, we delay the public announcement until the patch is available.
- If we find a previously unknown and unpatched vulnerability in software that is being actively exploited (a "0day"), we consider more urgent action - within 7 days - to be appropriate. The reason for this particular designation is that with each day that an actively exploited vulnerability is not disclosed to the public and unpatched, more devices or accounts are compromised. Seven days is an aggressive timeline and may be too short for some vendors to update their products, but it should be enough time to publish notices of possible remediation, such as temporarily disabling a service, restricting access, or contacting the vendor for more information. If 7 days have passed without a patch or notice, we will assist researchers in providing details so that users can take measures to protect themselves.
- If devices or software subject to the disclosure process are specifically designated by the manufacturer as end-of-life or end-of-support, we will limit the period to 30 days unless we receive positive confirmation that an out-of-band patch will be issued by the manufacturer.
- As always, we reserve the right to advance or shorten deadlines due to extreme circumstances. We remain committed to treating all vendors equally.

Châtelstrasse 5, CH-8355 Aadorf, Switzerland

We may contact international Computer Emergency Response Teams (CERTs [1]) or the National Cyber Security Center (NCSC[2]) during the responsible disclosure process to coordinate disclosure if critical vulnerabilities have been identified that affect a large user base or critical ICT systems.

1.3 Cooperation with software or hardware manufacturers

CRYPTRON Security Research Lab is committed to making reasonable efforts to establish communication with the affected manufacturer. We attempt to use the publicly available security contact, otherwise we contact vendor support via publicly available mechanisms and/or send emails to security@, support@, info@ addresses.

We ask vendors to provide an appropriate security contact, including encryption certificates, to protect the confidentiality of the security notice or any other communication.

In no case will a security vulnerability be "hidden" because a product vendor does not want to fix it. To keep the process transparent, we include the summary of communications with the vendor in the notice.

We encourage vendors to provide us with updated information that will be included in the final security notice. This could include: the software versions or hardware versions affected by the bug, the number of the fixed version, and a way to obtain the update (e.g., the URL of a website from which the security update or new version can be downloaded). We recommend that the vendor request the CVE numbers for the relevant vulnerabilities.

We welcome vendors to name the researcher(s) who identified the security issue and the CRYPTRON Security Research Lab in release notes and announcements.

CRYPTRON Security Research Lab

The CRYPTRON Security Research Lab is the integrated research facility of CRYPTRON Security GmbH, located in Switzerland. For inquiries, feedback, or comments, please contact info@cryptron.ch.

Securitytxt.org (RFC 8615) defines a standard that helps organizations define the process for security researchers to safely disclose security vulnerabilities. Security.txt files have already been adopted by Google, Facebook, GitHub, the UK government, and many other organizations. The CRYPTRON Security Research Lab also uses a security.txt file at the following link https://www.cryptron.ch/files/Cryptron/.well-known/security.txt.

[1] Computer emergency response team
[2] https://www.ncsc.admin.ch/ncsc/de/home.html