**Broadcom**
3421 Hillview Ave
Palo Alto, CA 94304
**broadcom.com**

# FAQ: Adapting to AI-Accelerated Vulnerability Discovery

### How is Broadcom's Infrastructure Software Group addressing the accelerated pace of vulnerability discovery and exploitation?

Broadcom Infrastructure Software Group is working to integrate frontier AI models as part of its vulnerability management programs, both within our own environments and within the products our Infrastructure Software Group delivers to customers. As with any security testing activities, when vulnerabilities or other flaws are uncovered, we address them through our standard remediation processes, using risk-based prioritization, and we deploy fixes along with appropriate communications. Those processes iterate constantly in response to changes in volume and velocity.

### Is Broadcom part of Anthropic's Project Glasswing to test its Mythos AI model?

Yes, as noted in Anthropic's public announcement of the project, Broadcom is a trusted participant in the model evaluation, which is being conducted pursuant to a Non-Disclosure Agreement.

### Do cybersecurity-trained AI models make Broadcom's software more secure or more vulnerable?

We believe AI will lead to a net improvement in the security of software provided by leading vendors like Broadcom insofar as it will likely accelerate the identification and prioritization of vulnerabilities, improve coding practices, and speed the timeline for deployment of security updates and patches. To learn more about what we have found to date by applying frontier AI security models to our own code, read our blog post.

### Will remediation timelines change?

Broadcom's vulnerability management practices are based upon severity and exploitability within the context of our products. Applicable fixes are included in appropriate release vehicles, including emergency patches and maintenance releases. Frequency of patches will continue to align with risk-based prioritization and industry practices.

### How will Broadcom customers know they need to patch or update?

Broadcom has existing communication mechanisms in place to communicate vulnerability disclosures and patch releases to our customers. We recommend all customers subscribe to the Broadcom security alerts for the products in use within their organization, as well as the appropriate patch announcement channels.

### Can you tell us about any newly discovered risks associated with Broadcom products or services?

Whenever a vulnerability is found within a Broadcom product or service, we follow responsible disclosure practices. These practices include considering the necessity and timing of any disclosure, the availability of a patch or mitigation, and the existence of any known public exploit. Providing more

specific details about any particular vulnerability would be outside of our responsible disclosure practices and create unnecessary risk for customers and end-users of our technologies.

**How can I learn more about this topic?**

We do not plan to update or revise these FAQs, whether as a result of changes in our practices, new information, future events or otherwise. However, you can reference Knowledgebase Articles, the Broadcom Support and Maintenance Handbook and the Customer Support Portal for further updates.